Draft Working Document

September 1999 **ISO TC215/WG2 - Report**

Electronic Healthcare Message Communication -

Essential Characteristics Required to Enable Precise Healthcare Messaging And Communication Standards

Version 1.03 dhm/gld

CONTENTS

Foreword

This International Standards Organisation [3.49] (ISO) Report has been prepared by ISO/TC215 Working Group 2 Healthcare Messaging and Communication.
This ISO Technical Report complies with the third edition of ISO/IEC Directives, part 3, 1997.
All annexes of this ISO Report are informative.

Introduction

The use of data processing and telecommunication capabilities have made possible the interchange of information in machine-readable and machine processable formats. The Information Technology and Data Management environment consists of a variety of computer systems with numerous hardware and operating system platforms. Application programs span a wide range of qualities of design and of support. They include user written applications, applications where the supplier has ceased to trade, and applications where the design and documentation is so poorly written and understood, they cannot be satisfactorily modified.

Interoperability – the ability of software and hardware on multiple machines from multiple vendors to communicate – is the key to automated interchange of information in healthcare. [3.31] As interoperability increases, it is essential to provide appropriate information interchange standards [3.59]. Electronic messages [3.44] developed in the Health Informatics domain contain sensitive healthcare information about specified individuals that requires a high level of confidence both in the parties sending and receiving messages and that the information being made available is unchanged.

Any implementation of information exchange should therefore include a security [3.58] profile including data protection and confidentiality [3.18] principles that, according to analysis of the local environment and national legislation, provide mechanisms to ensure proper levels of authentication [3.9], confidentiality, integrity [3.40] and availability. Whilst the development of the actual healthcare message itself must remain with experts in the specific field of activity, there is in addition a need to have available a ‘generic envelope’ to encompass healthcare messages and thereby ensure safe date flows.

The General scope of Activity agreed for Working Group 2 of ISO/TC215, includes the statement that

> “Any messaging and communication standard, or data interchange standard offered for consideration by the Working Group should include:
> - The functional purpose of the interchange and the circumstances in which the interchange should occur
> - An abstract definition of the interchange or message that identifies the concepts to be communicated and the data elements necessary to represent those concepts in the interchange
> - A means of implementing that interchange in one or more syntaxes or communication modalities”.

Implicit in this Scope statement is the stewardship of health information interchange and a fiduciary responsibility to the various constituent parties to that interchange. This **Trust Constituency** will rely substantially on WG2 and its work products to protect and engage in rights and obligations with regard to health information interchange.

The success of WG2’s work will ultimately be measured by industry acceptance of its products. A critical starting point, is the need to cultivate a bond of confidence, culminating in a trusted relationship, with its diverse constituency. Key factors supporting this alliance will be the advancement of ISO standards, which define, promote and ensure:

- **Trust:** confidence, surety.
- **Trusted Health Record Protection and Assurance**: privacy, confidentiality, stewardship, rights, Obligations.
- **Trusted End-to-End Information Flow**: point of origin (point of service/care) to point of use.
- **Security, Access Control.**
- **Accountability.**
- **Scope:** domain.
- **Functionality; Application, Interoperability, Tight Coupling**

- **Suitability: fit, finish.**
- **Controllability, Adaptability, Localization.**
- **Performance**
- **Data Integrity:** accuracy, context, consistency, comparability, continuity, completeness, relevance.
- **Persistence,**
- **Faithfullness**
- **Flexibility**
- **Validation**

It is imperative that the **Essential characteristics** of messaging and communication standards be identified on the requirements of implementers and end users (healthcare professionals). Each syandard originating from WG 2 and proposed for ISO adoption should be benchmarked against a formal set of Essential Characteristics.

The section 'Normative definitions and abbreviations' sets out a list of terms and definitions – the first use of a term in the text of the Report, carries a numerical reference to this Section.

This Report is set out in two Parts and an Annex:

Part I: Essential Characteristics: to be reviewed in developing the 'generic envelope'.

Part II: Essential Attributes [3.7]: included as an informative guide for implementers in the healthcare domain at large.

Annex A: An Exercise to Validate the Essential Characteristics Set Out in The ISO Technical Report

Scope

The Essential Characteristics of messaging and communication standards, are identified being based on the requirements of standards developers, implementers and end users [3.62] (e.g., healthcare professionals [3.37]). These Essential Characteristics form the architectural tenets and fundamental milestones of the Work Plan necessary to produce an implementable healthcare message. This Report specifies a framework of Essential Characteristics required to:

- Aid standards developers through establishing benchmarks and clear targets
- Aid standards implementers identify relevant issues in their specific domain
- Aid the identification of supplementary standards to be incorporated thus ensuring quality, uniformity and completeness of implementation
- Aid and identify inadequacies of existing standards

The products developed will protect and encompass the fiduciary responsibility of the various constituents parties through incorporating the rights and obligations required for such health information interchange. The Scope of the Work Plan is based on a statement of fundamental principals and objectives, including the following 14 elements:

1. Ensured Trust [3.61]

Constituent parties - individuals, organizations and business units - have a trust stake with regard to the veracity of the health record, including its origin, amendment, stewardship and use. With particular reference to:

1.1. Privacy and confidentiality;
1.2. Protection of individually identifiable information;
1.3. Protection during the course of interchange - “in transit”.

2. Trust Constituency

See relationships of constituent parties, Table 1 following "The Trust Constituency". There are a multitude of constituent parties to the health record and its content, each with definitive rights and obligations:

2.1 As subjects of the health record, e.g.:
(1) Individual subjects of care, health plan members;
(2) Individual healthcare professionals/caregivers;
(3) Individual originators of record content: authors, scribes and verifiers;
(4) Organizations, including: providers, health plans;
(5) Business units, including: departments, services, specialities;
(6) Others, including: next of kin, carers, emergency contacts, payment guarantors [3.53];

2.2. As parties participating in the provision, performance and completion of healthcare services who’s related actions are ascribed in the health record, e.g.:
(1) Individual Healthcare professionals/caregivers;
(2) Organizations;
(3) Business units;

2.3. As parties participating in the origin, amendment, stewardship and use of the health record whose related actions are ascribed therein, e.g.:
(1) Individual healthcare professionals/caregivers;
(2) Individual authors, scribes and verifiers;
(3) Organizations;
(4) Business units.

Constituent parties, in terms of the health record and its content, designated variously by local legislation, regulations, standards of practice and custom, are outside the Scope of this Report.

Trust Constituency: for health record content, including individually identifiable information Constituent	Individual	Organization	Business Unit	Subject of Record	Accountable Source, Author of Record Content	Accountable Verifier of Record Content	Accountable Scribe of Record Content	Accountable User of Record Content	Accountable Record Steward	Accountable Provider of Health Services as Documented in Record
Subject of care[3.60], Health Plan Member	X			Yes	Yes	A/A	N/A	A/A	No	No
Next of Kin, Emergency Contact	X			Yes	No	No	No	No	No	No
Healthcare Professional, Caregiver	X			Yes	Yes	Yes	Yes	Yes	Yes	Yes
Transcriptionist	X			Yes	No	A/A	Yes	A/A	Yes	No
Department, Service, Specialty			X	Yes	N/A	N/A	N/A	Yes	Yes	Yes
Provider	X	X		Yes	N/A	N/A	N/A	Yes	Yes	Yes
Integrated Delivery Network[3.47] (IDN)		X		Yes	N/A	N/A	N/A	Yes	Yes	Yes
Payment guarantor, Health Plan, HMO		X		A/A	No	No	No	Yes	Yes	No
Value Added Network (VAN)		X		No	No	No	No	Yes	Yes	No
Employer	X	X		A/A	No	No	No	Yes	A/A	No
Public Health Agency		X		No	No	No	No	Yes	A/A	No
Regulatory Agency		X		No	No	No	No	Yes	A/A	No
Accreditation Agency		X		No	No	No	No	Yes	A/A	No
Research	X	X		No	No	No	No	Yes	A/A	No
Professional Education	X	X		No	No	No	No	Yes	A/A	No
Others										

N/A = Not applicable A/A = As applicable

Table 1: Relationships Within The Trust Constituency

3. Health Record Rights

Health record rights include authentic information, which is complete, accurate and can be accessed by the record subject. Other crucial record rights include:

3.1. Confidentiality and privacy protections, particularly with regard to access to, use and disclosure of:

(1) Individually identifiable information;

(2) Information subject to protection:

a) by statute, regulation, standard of practice or custom; and/or

b) by virtue of explicit disclosure grants and agreements;

(3) Information made available by such grants and agreements:

a) for purpose(s) intended;

b) by those parties so authorized;

c) for the period (of time) designated; and

d) based on the principle of "need to know" [3.46].

3.2. Complete and accurate portrayal of health status and interventions;

3.3. Complete and accurate portrayal of the provision, performance and completion of health services;

3.4. Detailed audit logs tracking record creation, amendment, access, use and disclosure.

Health record rights designated variously by local legislation, regulation, standards of practice and custom, are outside the Scope of this Report.

4. Health Record Obligations

Health record obligations include accountability for:

4.1. record content origination and amendment, as ascribed to authors, scribes and/or verifiers;
4.2. provision, performance and completion of health services, as documented in the record and as ascribed to healthcare professionals, caregivers;
4.3. accuracy, completeness of record content;
4.4. access to, and use of, record content;
4.5. duplication of record content;
4.6. disclosure, transmission and receipt of record content;
4.7. translation of record content (e.g., mapping to alternate coding and classification schemes).

Health record obligations designated variously by local legislation, regulations, standards of practice and custom, are outside the Scope of this Report.

5. Health Record Composition

In its fullest manifestation, the health record (of the subject of care) comprises:

5.1. a longitudinal chronology of subject of care health status and interventions;
5.2. a chronicle of health service events corresponding to the provision, performance and completion of healthcare services;
5.3. a collection of discrete record instances (documents), often corresponding in a 1:1 relationship with health service events.

6. Healthcare Parties and Their Accountable Actions

Healthcare parties are those individuals, organizations and business units accountable for actions related to, and/or ascribed in, the health record, including:

6.1. Origination or amendment of record content: as authors, scribes, verifiers;
6.2. Provision, performance and/or completion of healthcare services, specifically health service events;
6.3. Access to, and use of, record content;
6.4. Duplication of record content;
6.5. Disclosure, transmission and/or receipt of record content;
6.6. Translation of record content.

In many but not all cases, individuals as healthcare parties, act as agents/employees and/or on behalf of organizations and business units.

7. Healthcare Agents [3.32] **and Their Accountable Actions**

Healthcare agents include medical devices (e.g., instruments, monitors) and software (e.g., applications, components) accountable for actions related to, and/or ascribed in, the health record, including:

7.1. origination of record content (typically pre-verification);
7.2. duplication of record content;
7.3. transmission and/or receipt of record content;
7.4. translation of record content.

Healthcare agents typically act within the domain, on behalf of and under the immediate control, of healthcare parties (as described above).

8. Scope of Accountability, Unit of Accountability

Accountable actions of healthcare parties, healthcare agents engage a corresponding scope of accountability. Such scope includes (the domain of) health record content ascribed to:

8.1. Healthcare parties in terms of their specific actions in the provision, performance and/or completion of health services;
8.2. Healthcare parties and agents in terms of their specific actions in the origination, amendment, stewardship and use of the record.

The scope of accountability can be reduced to a discrete unit of accountability, comprising a set of attributes (data elements):

8.3. describing the performance, provision and/or completion of a discrete health service event;
8.4. comprising a discrete record instance.

9. Authentication, Attestation, Non-Repudiation [3.48]**, Digital Signature** [3.24]

Authentication is fundamental to the trusted interchange of healthcare information. It enables a recipient to reliably verify the parties to the origination, validation, transmittal and receipt of health records, in whole or in part. Specific authentication functions are crucial, these include:

9.1. user authentication: evidence of individual identity;
9.2. source authentication: evidence of authorship, origination, amendment;
9.3. validation authentication: evidence of data verification, e.g.:
  (a) of data originated by another party;
  (b) of automated device input;
9.4. data interchange authentication: evidence of transmittal, receipt.

Other crucial aspects of authentication include:

9.5. non-repudiation (e.g., of authorship);
9.6. attestation;
9.7. digital signature;
9.8. public[3.55]/private key[3.54] infrastructure;
9.9. encrypted encapsulation: binding record content to an authenticated source.

10. Auditability

Intrinsic to full accountability is the establishment of robust audit trails [3.8] and audit tools, sufficient to comprehensively track healthcare parties and agents and their accountable actions (as described in the preceding sections).

11. Chain of Custody

As end-to-end information flows imply, there is an intrinsic need to track the chain of custody as health records transit points of interchange, points of translation and points of convergence.

12. Faithfulness, Permanence, Persistence and Indelibility

Another pre-requisite is the need to ensure health records are faithfully maintained in a permanent, indelible, unaltered form, from point of origination to point of use. This includes:

12.1. preservation of original content and context;
12.2. revision by (additive) amendment only;
12.3. preservation of discrete data states: for the original and each amendment;
12.4. ability to reconstruct health records for any given historical date/time.

13. Data Definition, Data Registry [3.57]

Concise data definition is the foundation to data integrity [3.21], including definitions of attributes (i.e., data elements) and data groups (e.g., minimum, core, and reference data sets). Data registries, such as the U.S. Health Information Knowledge base (USHIK), are a basic method to ensure the formalization and harmonization of attribute/data group definitions across SDOs, accreditation and governance bodies, and others.

14. Data Integrity

Significant aspects of data integrity include accuracy, context, consistency, comparability, continuity, completeness and relevance. Data integrity is based on data definition, as described above, but also relies substantially on robust methods for information flow from the point of origination to the point of use.

Consequent upon the above review, the Obligations and their Emphasis in Trusted Messaging and Communication Architecture are identified and set out in Table 2.

ISO IST/215 Report No.??? has a fiduciary duty to design or adopt architectures and interchange methodologies which:	Ensures trust in the veracity and Protection of health records to all Constituent parties **(Ensured Trust)**
	Recognises, ensures and protects the Incumbent interests of these Constituent parties (Major Stakeholders)**(Trust Constituency)**
	Recognises and ensures fundamental **Heath Record Rights**
	Recognises and ensures fundamental **Health Record Obligations**
	Allows the full representation of the **Health Record and its Composition**
	Allows full representation of **Healthcare Parties and Their Accountable Actions**
	Allows full representation of H**ealthcare Agents and Their Accountable Actions**
	Allows full representation of healthcare parties/agents, their actions and corresponding **Scope of accountability, Unit of accountability**
	Ensures and enables the full set of services for **Authentication, Attestation, Non-Repudiation, Digital Signature**
	Ensures **Auditability** of accountable parties/agents and their accountable actions with regard to the health record and its content
	Ensures **Chain of Custody** tracking in the course of information flow from the point of origin (e.g. The point of service care)to the point of use
	Ensures Faithfulness, Permanence, Persistence and Indelibility of the health record and its content
	Ensures robust methods **of Data Definition,** including formalization and harmonisation with recognised **Data Registries**
	Ensures vital aspects of **Data Integrity**

Table 2: Obligations to be observed in developing Trusted Messaging Communications Architecture

2.0 Normative References

The following normative documents contain provisions that, through reference in this text, constitute provisions of this ISO Report. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this ISO Report are encouraged to investigate the possibility of applying the most recent editions of the normative documents below. For undated references, the latest edition of the normative document referred to applies. Members of ISO and IEC maintain registers of currently valid International Standards.

ISO/IEC 7826-2:1994	*Information technology – General structure for the interchange of code values – Part 2: Registration of coding schemes.*
ISO/IEC Guide 1996	*Guide 2: definition 3.2*
ISO 2382-4	*Information processing systems – Vocabulary – Part 04: Organisation of data*
ISO 7493/2: 1989	*Systems Interconnection – Basic reference model – Security architecture*
ISO 6523: 1984	*Data interchange – Structure for the identification of organisations*
ITSEC	*Information Technology Security Evaluation Criteria. Published by the European Commission Version 1.3, 1992*
ENV 1613:1995	*Medical Informatics - Messages for exchange of laboratory information.*
ENV 12265:1996	*Medical Informatics – Electronic health record architecture*
ENV 12443: 1996	*Medical Informatics - Healthcare information framework*
HL7	*Health Level 7 Secure Transactions Special Interest Group December 1998*
OMG 97	*Object Management Group Publications 1997, Chapter 15*

3.0 Normative definitions and abbreviations

For the purposes of this ISO Report, the following definitions (listed in alphabetical order) apply:

3.1 access control
The prevention of an unauthorised [3.10] use of a resource, including the prevention of use of a resource in an unauthorised manner
[ISO 7498 – 2]

3.2 accountability
the property that ensures the actions of an entity can be traced uniquely to the entity
[ISO 7498 –2]

3.3 architecture
a set of principles on which the logical structure and interrelationships to an organisation and business context are based. It is the result of software design activity

3.4 archiving health records
the process of saving healthcare data [3.33]for later reference or use
[COACH]

3.5 assurance
development, documentation, testing, procedural, and operational activities carried out to ensure a system's security services do in fact provide the claimed level of protection
[OMG 97]

3.6 asymmetric cryptographic algorithm
An algorithm for performing encipherment or the corresponding decipherment in which the keys [3.42] used for encipherment and decipherment differ
[ISO 10191-1]

3.7 attribute
An identifiable association between an object and some other object or set of objects

3.8 audit trail
record of the resources which were accessed and/or used by whom
Note: This may involve a formal monitoring technique for comparison between the actual use of a medical information system and pre-established criteria.
[ISO 7498 – 2]

3.9 authentication
the process of reliably identifying security subjects by securely associating an identifier and its authenticator
[ISO 7498 – 2]

3.10 authorise
granting of rights, which includes granting of access based on access rights
[ISO 7498-2]

3.11 availability
the property of being accessible and useable upon demand by an authorised entity
[ISO 7498-2]

3.12 biometrics
the use of specific attributes that reflect unique personal characteristics, such as a fingerprint, an eye blood-vessel print, or a voice print, to validate the identity of entities
[ISO/IEC 2382-08]

3.13 certification
procedure by which a third party gives assurance [3.5] that all or part of a data processing system conforms to security requirements
[ISO/IEC 2382-08]

3.14 ciphertext
data produced through the use of encipherment. The semantic content of the resulting content is not available
[ISO 7498-2]

3.15 clearance
permission granted to an individual to access information at or below a particular security level
[ISO/IEC 2382-08]

3.16 clinical information
information about a subject of care, relevant to the health or treatment of that subject of care, that is recorded by or on behalf of a healthcare person
NOTE: Clinical information about a subject of care may include information about the subject of care's environment or about related people where this is relevant.
[CEN ENV 1613:1995]

3.17 coding scheme
collection of rules that maps the elements of one set on to the elements of a second set
[ISO/IEC 7826] [ISO 2382-1987, modified] [ENV 1068]

3.18 confidentiality
the property that information is not made available or disclosed to unauthorised individuals, entities or processes
[ISO 7498 – 2]

3.19 consent
voluntary agreement with what is being done or proposed (express or implied)
[GHH]

3.20 credentials
data that are transferred to establish the claimed identity of an entity
[ISO/IEC 2382-08]

3.21 data integrity
property that data has not been altered or destroyed in an unauthorised manner
[ISO 7498-2]

3.22 decision support
electronic system designed to aid healthcare professionals make clinical decisions

3.23 decryption
the process of obtaining, from ciphertext [3.14], the original corresponding data
Note: a ciphertext may be encrypted a second time, in which case a single decryption [3.23] does not produce the original plain text
[ISO/IEC 2382-08]

3.24 digital signature
data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data to prove the source and integrity of the unit. It protects against forgery, even by the recipient
Note: This term is usually reserved for digital values or checksums calculated using asymmetric techniques, where only the originator of the message can generate the digital signature but many people can verify it
[ISO 7498 –2]

3.25 EDIFACT
Electronic Data Interchange for Administration, Commerce and Transport. They comprise a set of internationally agreed standards, directories and guidelines for the electronic interchange of structured data. (Also referred to as UN/EDIFACT)

3.26 electronic health record
EHCR
Health record concerning the subject of care in computer readable form
[CEN prENV13606-1]

3.27 encryption
the cryptographic transformation of data to produce ciphertext
[ISO 7498 – 2]

3.28 episode of care
identifiable grouping of healthcare related activity characterised by the entity relationship between the subject of care and a healthcare provider [3.38], such a grouping determined by the healthcare provider

3.29 escrow
a written agreement deposited with a third party, setting out a manufacturer's/supplier's obligations as to the manner software source code and documentation are (when appropriate) to be made available to users

3.30 firewall
A computer system providing an isolation layer between a private network security domain and a public untrusted network
[CIHI]

3.31 healthcare
provision of health related services
Note : This includes ,more than performing procedures on subjects of care. It includes also e.g. the management of

[CEN TC/251 PT30]

3.32 healthcare agent
healthcare person, healthcare organisation [3.35], healthcare device or healthcare software component that performs a role in a healthcare activity
[CEN ENV12265, modified]

3.33 healthcare data
data which are input, stored, processed or output by the automated information system which support the business functions of a the Healthcare organistion. These data may relate to person identifiable records or may be part of an administrative system where persons are not identified.
[HL7]

3.34 healthcare informatics
Scientific discipline that is concerned with the cognitive, information processing and communication tasks of healthcare practice, education and research, including the information science and technology to support these tasks
[Directory of the European Standardization Requirements for Healthcare Informatics and Telematics (version 2.1 1996.08.15)]

3.35 healthcare organisation
organisation involved in the direct or indirect provision of healthcare services to an individual or to a population or in the provision of healthcare related services
Examples: general medical practitioner's surgery/clinic, community pharmacy, hospital
NOTE 1 Groupings or subdivisions of an organisation, such as departments or sub-departments, may also be considered as organisations where there is need to identify them.
Note 2 Modified from CEN ENV1613:1995

3.36 healthcare party
organisation or persons involved in the direct or indirect provision of healthcare services to an individual or to a population or involved in the provision of healthcare related services
Note 1: organisations responsible for the funding, payment, or reimbursement of healthcare provision are healthcare parties
Note Modified from CEN ENV 1613:1995

3.37 healthcare professional
person is entrusted with the direct or indirect provision of defined healthcare services to a subject of care or a population of subjects of care
Examples: qualified medical practitioner, pharmacist, nurse, social worker, radiographer, medical secretary or clerk
[CEN ENV 1613: 1995]

3.38 healthcare provider
healthcare organisation or healthcare professional responsible for the direct provision of healthcare to a subject of care
Note: organisations responsible for the funding, payment, or reimbursement of healthcare provision are not healthcare providers
[CEN TC/251 PT30]

3.39 inpatient
subject of care who is admitted to a healthcare organisation for overnight stay, in order to receive health care

3.40 integrity
the property that data or a message's content has not been altered or destroyed in an unauthorised manner
Note 1: In order to achieve this requirement for the data, the integrity of all system assets, must be preserved

Note 2: This definition includes both accidental and intentional events and actions
[ISO 7498 –2]

3.41 interface
may be both physical, electrical and logical. A hypothetical junction being a process that permits the flow of data from one system to another in a structured manner
Note: This term can be used with a qualifier to describe an attribute to allow data flow to take place over this point.

3.42 key
A sequence of symbols that controls the operations of encipherment and decipherment
[ISO 7498-2]

3.43 linkage
the purposeful combination of data or information from one data processing system with data or information from another system to derive protected information
[ISOIEC 2382-08]

3.44 message
an identified and structured set of data elements and segments covering the requirements for a specified transaction

3.45 message standard
the sequence, attributes and usage of data elements within a message

3.46 need-to-know
a legitimate requirement of a prospective recipient of data to know, to access, or to possess any sensitive information represented by these data
[ISO/IEC 2382-08]

3.47 network
an electronic data transmission facility which can comprise of just a point to point wire link between two devices, or a complex arrangement of transmission lines

3.48 non-repudiation (of origin, of submission, of receipt)
a security service providing the recipient with proof that the message origin is as claimed, the message has been submitted to the Message Handling Service, the message has been delivered by the MHS or that the intended receiver of the message has received and read the message

3.49 organisation
unique framework of authority within which a person or persons act, or are designated to act towards the same purpose.
Note: groupings or subdivisions of an organisation may also be considered as organisations where there is need to identify them for information interchange
[ISO 6523:1984]

3.50 outpatient
subject of care whose episode of care [3.28] in a healthcare organisation does not require an overnight stay in that same organisation

3.51 patient (subject of care)
subject of care who is the subject of healthcare activity

3.52 password
confidential authentication information composed of a string of characters
[ISO 7498 – 2]

3.53 payment guarantor
individual or organisation responsible for the total or partial reimbursement or payment for the provision of healthcare services

Examples: subject of care, insurance company
[CEN prENV 1307]

3.54 private key
a key that is used with an asymmetric cryptographic algorithm [3.6] and whose possession is restricted (usually to only one entity)
Note: This key may be used for decryption or signature generation
[ISO 10181-1]

3.55 public key
a key that is used with an asymmetric cryptographic algorithm and can be made publicly available
Note: This key may be used for encryption [3.27] or signature verification
[ISO 10181-1]

3.56 recovery
the restoration of an information system back to an error-free and secure state from which normal operation can resume
[CEN]

3.57 registry
a server capable of holding data for the systematic and continuous follow up of information objects maintained in accordance with specific rules

3.58 security
the combination of security properties (such as availability [3.11], confidentiality, integrity and accountability) that constitutes a guarantee that data items and, more generally, any kind of security object has not been altered, modified, disclosed, or withheld by any kind of security subject in an unauthorised manner with respect to the security policy
[ITSEC]

3.59 standard
document, established by consensus and approved by a recognised body, that provides, for common and repeated use, rules, guidelines, or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context
Note: Standards should be based on the consolidated results of science, technology and experience, and aimed at the promotion of optimum community benefits
[ISO/IEC Guide 2: 1996]

3.60 subject of care
person or defined groups of persons receiving or registered as eligible to receive healthcare services or having received healthcare services
Examples: patient
[CEN ENV 12443:1996]

3.61 trust
reliance on the integrity, justice etc of a person, or on some quality or attribute of a thing

3.62 user
a person or other entity authorised by a provider to use some or all of the services provided by the provider
[COACH]

3.63 ABBREVIATIONS

The following abbreviations are used for the terms defined in this ISO Report.

DICOM	Digital Imaging and COmmunications in Medicine; standard developed by ACR/NEMA
CEN	Comite' Europeen de Normalisation
CIHI	Canadian Institute for Health Information
COACH	Canadian Organisation for the Advancement of Computers in Health (now Canadian Health Informatics Association)
E C	Essential Characteristics
EDI	Electronic Data Interchange
ENV	European pre-standard
HL7	Health Level Seven Interface[3.41] Standard; an American National Standards Institute (ANSI) Accredited Standards Developing Organisation
ISO	International Standardization Organisation
ISO TC/215	ISO Technical Committee (215) Healthcare Informatics[3.34]
ITSEC	Information Technology Security Evaluation Criteria

Part I: Essential Characteristics

The relevance of this Report is based on an ability to capture all of the foreseen needs of the various healthcare constituent parties to information exchange. Whilst appearing to be overly complex, Part I provides the implementer/user with a comprehensive list from which they can be selective in developing a standard suitable for their needs. It is also intended to aid implementers/users in achieving a deeper understanding of the 'standards process' and thereby assist in accomplishing the aims and requirements of the message standard [3.45]. Whilst this listing is intentionally extensive, it is not exhaustive and must not be considered to be a final solution.

The following sections outline the proposed Essential Characteristics to support the Principles and Objectives for healthcare messaging and communications standards, as set out in the Scope of this Technical Report. Essential Characteristics are designed to represent the needs of the healthcare community: e.g., the subject of care; the healthcare professional/caregiver; the healthcare business unit; the organization; the integrated delivery network.

The applicability of any Essential Characteristic to a messaging/communication standard corresponds:

- To the interchange role (of the standard);
- To its designated domain of information and interchange interactions;
- To the anticipated behaviour of the communicant applications, components or devices it serves, etc.

A given standard may be positioned (fit) amongst other standards which when joined collectively, provide an array of Essential Characteristics (EC).

1. Identifiable Information

(1A) Interchange of Identifiable Information
This messaging/communication EC specifies the interchange of health records or information which may be identifiable to specific healthcare parties (i.e., individuals, organizations, business units), and/or which may include their distinguishing traits.
Examples: where information identifiable to an individual party may be interchanged:

- Information interchange between multiple front-end clinical applications to manage the real-time health delivery process and work flow.
- Information interchange from clinical front-end applications to back-end repository.
- Information interchange to third parties (e.g., payors for claims, public health agencies for immunization, communicable disease registries).

2. Architectural Basis

(2A) Architectural Basis
This messaging/communication EC is based on a formalized architecture.
Example:

- Architectural template for interchange of information among and between multiple clinical, administrative and operational applications in a healthcare provider enterprise or integrated delivery network.

3. Master Files

(3A) Master Files – In General
This messaging/communication EC specifies the interchange of master file definition information.
Example:

- Synchronous master file updates via interchange among all applications serving a health provider enterprise.

(3B) Master File: Data Definition
This messaging/communication EC specifies the interchange of information sufficient to enable data definition

(3C) Master File: Context Sets/Templates

This messaging/communication EC specifies the interchange of information sufficient to enable context set/template definition. Context sets are specializations of data groups for particular aggregation purposes.

Examples:

- Templates, which encapsulate evidence of vital contexts regarding a clinical service event.
- Templates, embedded in trusted end-to-end information flows, from point of origination (point of service/care) to point of use.

(3D) Master File: Function Definition

This messaging/communication EC specifies the interchange of information sufficient to enable application function definition and corresponds to the granularity of security classifications (in the following section).

Example:

- For the healthcare professional: application functions which access, manage or process information: e.g.,
  - Access/review subject of care health record;
  - Create or activate clinical encounter;
  - Update, hold or discharge clinical encounter;
  - Create, amend order for clinical service(s);
  - Schedule clinical service event(s);
  - Perform or complete clinical service event(s);
  - Hold or cancel clinical service event(s);
  - Archive health records.

(3E) Master File: Security Classification Definition

This messaging/communication EC specifies the interchange of information sufficient to enable security classification definitions.

Examples:

- Classifications, which protect the confidential content of the subject of care health record, at designated levels of sensitivity, and based on, e.g.:
  - Accountable roles;
  - Need to know.
- Classifications, which protect the confidential content of an organizations business (operations), record.
- Classifications which protect the confidential content of a healthcare professional's service record.
- Classifications, which control access to individually identifiable health information, to health records, to review functions.

(3F) Master File: Security Clearance[3.15] Definition

This messaging/communication EC specifies the interchange of information sufficient to enable security clearance definitions.

Example:

- User clearances which permit access to sensitive and protected information based on:
  - Accountable healthcare roles;
  - Need to know.

(3G) Master File: Security Policy Domain Definition

This messaging/communication EC specifies the interchange of information sufficient to establish and maintain one or more security policy domain definitions. Across a business unit, organization or broader network, a security policy domain enables access policies and ensures uniform access control [3.1], to information and functions.

Examples:

- Policy domain(s) which may be applicable to discrete business units, an entire health provider enterprise or integrated delivery network.
- Policy domain(s) which may be applicable to specific sets of health record information (e.g.,

(3H) Master File: Orders, Order Sets
[…]

(3I) Master File: Services, Service Events
[…]

(3J) Master File: Work Flow
[…]

(3K) Master File: Protocols (Care Plans, Critical Paths)
[…]

(3L) Master File: Decision Support Rules, Conditions, Actions
[…]

(3M) Master File: Facilities, Locations
[…]

(3N) Master File: Resources
[…]

(3O) Master File: Charges, Costs
[…]

4. Master Registries

(4A) Master Registry: Accountable Healthcare Parties
This messaging/communication EC specifies the interchange of registry information sufficient to enable a master registry to be constructed of accountable healthcare parties, including individuals, organizations and business units.
Each accountable healthcare party [3.36] may be known by 1-n identifiers, may be assigned 1-n healthcare roles and may be afforded access privileges under 1-n security clearances
The information content of this registry (may) include: personal identifiers, demographics, contact information, licenses/credentials [3.20], role(s), security clearance(s), access details (e.g., passwords [3.52], biometrics) [3.12], affiliations (e.g., practice group, organization, business unit (department, service, specialty)), privileges, activation status, etc.
Example:
- A master registry of healthcare professionals, caregivers and system users for a healthcare provider enterprise, for an integrated delivery network.

(4B) Master Registry: Accountable Healthcare Roles
This messaging/communication EC specifies the interchange of registry information sufficient to enable a master registry of accountable healthcare roles, particularly with regard to:
- Provision, performance and/or completion of health services;
- Origination, amendment, stewardship and use of the health record.

Each role may be afforded access privileges under one or more security clearances.
Examples:
- Attending physician, resident, registered nurse, respiratory therapist, pharmacist, clinical consultant, physician's assistant, transcriptionist, clerk…
- Including specialists: radiologists, pathologists, cardiologists…

(4C) Master Registry: Accountable Healthcare Agents
This messaging/communication EC specifies the interchange of registry information sufficient to enable a master registry of accountable healthcare agents, including devices and application software.
Examples:
- Devices: bedside monitors, ventilators, IV pumps, lab instruments, dispensing devices…

- Software: bedside, laboratory, radiology, pharmacy, reg/ADT, order entry, scheduling, workflow, medication dispensing and administration, nursing…

(4D) Master Registry: Persons (Health Subjects)
This messaging/communication EC specifies the interchange of registry information sufficient to enable the construction of a master registry of individual subjects of care and health plan members.
Examples:
- Registry of persons served by a healthcare provider enterprise, by a health plan, by an integrated delivery network.
- Registry of persons receiving clinical services.

(4E) Local Identifier Assignment
This messaging/communication EC specifies the interchange of information sufficient to enable and track local identifier assignment.
Examples:
- Subject of care/health plan member ID: e.g., medical record number
- Healthcare professional, employee, user ID
- Encounter, episode ID
- Financial account ID
- Location ID
- Equipment, property tag/ID
- Local product ID

5. Electronic Records

(5A) Personal Health Record
This messaging/communication EC specifies the interchange of the personal health record and its subsets.
The personal health record chronicles the health status and interventions for an individual subject of care.
The information content of the personal health record (may) include: personal identifiers and demographics, environmental, social, financial (e.g., healthcare coverage), allergies, clinical interventions, problems/episodes of care, visits/encounters, personal schedule, consents[3.19], disclosures, services received, medication profile, audit, etc.
Example:
- Subject of care-centered electronic health record system serving a health provider enterprise or an integrated delivery network.

(5B) Population Health Record
This messaging/communication EC specifies the interchange of information related to a population health record. A population health record may comprise the aggregation or summaries of many personal records and may not contain information individually identifiable or selectable.
Example:
- Extractions, aggregations and summaries for performance, quality assurance and outcome reporting, utilization, public health, epidemiology, clinical research, etc.

(5C) Business (Operations) Record
This messaging/communication EC specifies the interchange of information related to a business record. A business record defines and chronicles the operations of an organization or business unit, including services performed/provided and current status. It may or may not contain information individually identifiable or selectable.
Example:
- The business (operations) record and its subsets: policies, procedures, standards of practice/care, guidelines, schedules, allocations, deployments, assigned responsibility, work flow, performance, compliance, utilization, productivity, quality assurance, costs, services rendered, outcomes, audit, legal, etc.

(5D) Personal Healthcare Professional Service Record
This messaging/communication EC specifies the interchange of information related to a personal healthcare professional service record.
A personal service record chronicles assignments and services performed/provided by an individual healthcare professional/caregiver, including current status.
Example:

- The personal service record and its subsets: assigned responsibility, personal schedule, services rendered, audit, etc.

(5E) Multi-Media Record
This messaging/communication EC specifies the interchange of information in multiple media formats.
Example:

- Electronic health record[3.26] complete with multi-media content.

6. Record Chronology, Continuity, Completeness

(6A) Chronological Order of Events
This messaging/communications EC specifies the interchange of information sufficient to describe a chronology of events and corresponding records, for:

- Personal health record
- Population health record
- Business (operations) record
- Personal healthcare professional service record

Examples:

- Longitudinal subject of care health record.
- Business operations log.
- Time-based population study extracts for clinical or outcomes research.
- History of subject of care contacts for a healthcare professional (e.g., to ascertain exposure to infectious disease).

(6B) Event Timeline
This messaging/communications EC specifies the interchange of information sufficient to describe an event timeline.

- Prospective (future): events scheduled, not yet underway
- Concurrent (now): events in progress, not yet completed
- Retrospective (historical): events completed, in terminus state

Examples:

- Health history for an individual subject of care.
- Health service events in progress, not yet complete.
- Forthcoming health service events including well-being checks.

(6C) Historical Snapshot
This messaging/communications EC specifies the interchange of information sufficient to recreate the state of the health delivery process and the health record (or subset thereof) for an historical date/time.
Example:

- Snapshot of the personal health record at the moment of a critical clinical decision, viewed after the fact.

(6D) Continuity, Completeness
This messaging/communications EC specifies the interchange of information sufficient to ensure the continuity and completeness of the health record.
Example:

- Encounter-oriented health record completion summary:
  - What's incomplete?
  - Who's responsible?
  - Is it ready to close?

- Can it be final billed?

7. Authentication, Non-Repudiation Services

(7A) User Authentication.
This messaging/communications EC specifies the interchange of information sufficient to ensure user authentication, including evidence of identity of accountable healthcare parties and their accountable actions.
Example:
- Trusted identity of users, healthcare professionals, caregivers.

(7B) Data Source Authentication
This messaging/communications EC specifies the interchange of information sufficient to ensure data source authentication, including evidence of identity of accountable healthcare parties/agents and their accountable actions of authorship, or to originate or amend health record content.
Example:
- Trusted identity of health record content authors, scribes.

(7C) Validation Authentication.
This messaging/communications EC specifies the interchange of information sufficient to ensure verification authentication, including evidence of identity of accountable healthcare parties and their accountable actions to verify health record content.
Example:
- Trusted identity of health record content verifiers (e.g., content authored by another, input from an automated device).

(7D) Data Interchange Authentication
This messaging/communications EC specifies the interchange of information sufficient to ensure data interchange authentication, including evidence of identity of accountable healthcare parties and their accountable actions to disclose, transmit or receive health record content.
Examples:
- Trusted identity of transmitters and receivers
- Firewalls installed.

(7E) Non-Repudiation Services
This messaging/communication EC specifies the interchange of information sufficient to enable trusted non-repudiation services.
Example:
- Non-repudiation services for health record authorship, origination, amendment, verification, duplication, disclosure, transmittal, receipt.

8. Digital Signature

(8A) Digital Signature
This messaging/communications EC specifies the interchange of information sufficient to enable a robust digital signature methodology.
A digital signature binds the identity of an accountable healthcare party and affirmation of their accountable action(s) to health record content and/or to the performance, provision and completion of clinical service events. This binding establishes the scope of accountability.
Examples:
- Trusted attestation, affirmation of authorship of health record content.
- Trusted attestation, affirmation of responsibility for the performance or provision of healthcare services.

(8B) Public/Private Key Infrastructure (PKI)
This messaging/communications EC specifies a digital signature based on trusted certification [3.13] authorities and a public/private key infrastructure.

9. Audit

(9A) Audit Trails
This messaging/communications EC specifies the interchange of information sufficient to track the accountable actions of accountable healthcare parties.
Examples:

- Audit log showing the stream of events emanating from a laboratory service order: order, verify order, draw specimen, accession specimen, analyse specimen, post preliminary results, verify and sign final results, post final results, post supplemental or corrected results.
- Audit log showing the stream of events emanating from a radiology service order: order, verify order, schedule examination room, schedule subject of care NPO, transport subject of care, check subject of care into department/examination room, perform examination, check subject of care out, transport subject of care back to nursing unit, perform initial review of examination results, dictate preliminary report, transcribe report, review and revise report, transcribe revisions, review and sign final report, post final report.

(9B) Audit Review
This messaging/communications EC specifies the interchange of information sufficient to enable review of audit trail detail.
Example:

- Audit log showing users or healthcare professionals accessing the personal health record for subjects of care to which they are not assigned (e.g., fellow employees, celebrity cases).

10. Permanence, Persistence, Non-Alterability

(10A) Permanence, Persistence, Non-Alterability
This message/communications EC specifies interchange of information sufficient to ensure the permanence, persistence and non-alterability of the health record.
Examples:

- Trusted persistence of health record content unaltered from its point of origin to its point of use.
- Audit logs showing content at origin and with each successive amendment.

11. On-Line Transaction Processing (OLTP)

(11A) OLTP
Examples:

- Real-time, highly integrated electronic health record system encompassing a health provider organization and its business units, an integrated delivery network.
- Highly interactive electronic health record system, supporting prospective, concurrent, retrospective views of the health delivery process and health record chronology.
- Tightly coupled applications, components and devices.
- Synchronous data stores.

(11A) Tightly Coupled OLTP Services
This messaging/communications EC specifies tightly coupled interchange services sufficient to support real-time, high performance On-Line Transaction Processing (OTLP).

(11B) Multi-Phase Commit
This messaging/communications EC specifies tightly coupled interchange services sufficient to support multi-phase commits across synchronous data stores: e.g., bid, open/lock, update, close/unlock.

12. On-Line Analytical Processing (OLAP)

(12A) OLAP
Examples:

(operational) and clinical information[3.16].
- Executive information systems.

(12A) OLAP
This messaging/communications EC specifies the interchange of information sufficient to support On-Line Analytical Processing applications (e.g., a data warehouse).

13. Fault Tolerance

(13A) Fault Tolerance
Example:
- Fault tolerant architecture [3.3]supporting continuous runtime (i.e., 24x7x365), for a healthcare provider organization, for an integrated delivery network.

(13A) Redundant Communications Architecture
This messaging/communications EC specifies a redundant communication architecture sufficient to support fault tolerant interchange.

(13B) Unavailability/Failure Detection
This messaging/communications EC specifies a real-time failure detection architecture, sufficient to determine the non-operational (unavailable) status of communicant devices and applications.

(13C) Availability/Restart Detection
This messaging/communications EC specifies a real-time detection architecture sufficient to determine the operational (available) status of communicant devices and applications, including those just restarted.

(13D) Downtime and Slow Response Queuing
This messaging/communications EC specifies a message queuing scheme sufficient to buffer interchange in the case of downtime or slow response cycles between communicant applications and devices.

(13E) Recovery [3.56]
This messaging/communications EC specifies a method of post-downtime restart and recovery, in the case where one or more applications and/or devices have been unavailable for a period.

14. Data Synchrony

(14A) Data Synchrony
Example:
- Multiple applications or components with independent data stores requiring synchronization services, across a healthcare provider organization, across an integrated delivery network.

(14A) Data Synchronization
This messaging/communications EC specifies the interchange of information sufficient to ensure the logical synchronization of information and data stores across communicant applications, components and devices:
- At the initial binding
- At restart
- Continuously in normal operation

15. Time Synchrony

(15A) Time Synchrony
This messaging/communications EC specifies the interchange of information sufficient to maintain, within an agreed tolerance, time synchrony across communicant applications, components and devices:
- At initial binding

- At restart
- At routine intervals in normal operation

Example:

- Multiple applications or components requiring time synchronization services, across a healthcare provider organization, across an integrated delivery network.

16. Trusted End-to-End Information Flows

Examples:

- Assurance that health record content persists from its point of origin (point of service/care) to a specific point of use.
- Assurance of origination when, where and by whom indicated.
- Assurance of accountability and chain of custody.
- Assurance of data integrity.
- Assurance of essential clinical and operational context.
- Assurance of firewall integrity.

(16A) Trusted End-to-End Information Flows

This messaging/communications EC is based on an architecture sufficient to ensure trusted end-to-end information flows, from the point of origin (point of service/care) to the point of use. In the course of such flow, information may traverse:

- One or more points of interchange: i.e., interfaces between applications/devices
- One or more points of translation: e.g., where content is translated from one coding/classification scheme to another
- One or more points of convergence: e.g., where aggregation, derivation or summary may occur

(16B) End-to-End Record Audit

This messaging/communications EC specifies the interchange of information sufficient to reliably audit its flow from the point of origin to the point of use, tracking accountable actions of accountable healthcare parties/agents.

Examples:

- Audit log showing detailed record history: e.g., create record, verify and sign record, amend record, disclose/transmit record, translate record content, receive record, steward record, access/use record.

(16C) Chain of Custody Audit

This messaging/communications EC specifies the interchange of information sufficient to reliably track the health record or its subset from point of origination to point of use - effectively a chain of custody - including traversals of points of interchange and points of translation.

Example:

- Audit log with entries for each accountable healthcare agent in the chain of interchange.

(16D) Context Sets, Templates

This messaging/communications EC specifies interchange of information sufficient to enable context sets (templates) from the point of origination to the point of use.

Examples:

- Templates which persist from the point of record origin (point of service/care) to the point of use.
- Templates describing the essential context of a clinical service event:
  - Accountability Context, describing:
    - Who, what, when, where, why, how
  - Data Integrity Context, describing rules, measures and indicators for information/data:
    - Accuracy
    - Context
    - Comparability, consistency
    - Continuity, completeness
    - Relevance
  - Clinical Context, describing:
    - Rationale

- Clinical parameters
- Clinical context and conditions
- Measures of continuity and completeness (e.g., of the clinical service event)
- Measures of compliance (e.g., with standards of care/practice)
- Performance measures
- Quality indicators
- Outcome indicators

· Operational Context, describing:

- Allocation, deployment
- Assigned responsibility
- Resource utilization (e.g., for staff, time, facilities, equipment, supplies)
- Costs
- Productivity

17. Disclosure, Export

Examples:

♦ Assurance of controlled and authorized disclosure of personal health information, based on explicit permissions and need to know, to specified parties, for purposes/uses described.

♦ Audit logs of disclosures of health records and information.

(17A) Disclosure Authorization, Scope

This message/communications EC specifies interchange of information sufficient to track authorizations for disclosure.

(17B) Controlled Disclosure Tracking

This message/communications EC specifies interchange of information sufficient to track actual disclosure of sensitive or protected content.

(17C) Disclosure Labelling

This message/communications EC specifies interchange of information sufficient to ensure labelling of disclosed content as sensitive or protected, as applicable.

(17D) Dis-identification, Aliasing

This message/communications EC specifies interchange of information sufficient to ensure dis-identification or aliasing of data exports.

18. Prospective Services

(18A) Subject of Care Schedule

This message/communications EC specifies interchange of information sufficient to enable a prospective health schedule for subjects of care.

Example:

♦ Subject of care-centered enterprise-wide schedule.

(18B) Assigned Responsibility

This message/communications EC specifies interchange of information sufficient to enable assigned responsibility for scheduled clinical service events, based on business and clinical practice rules.

Examples:

♦ Assurance of known responsibility for performance, provision and completion of clinical service events.

♦ Assurance of known responsibility for completion of health record entries, as author, as scribe, as verifier.

(18C) Practitioner Schedule

This message/communications EC specifies interchange of information sufficient to enable a prospective schedule for healthcare professionals, caregivers, groups and roles.

Example:

- Healthcare professional-centered enterprise-wide schedule and work list.

(18D) Resource Schedule
This message/communications EC specifies interchange of information sufficient to enable a prospective resource-based schedule.
Examples:
- Resource oriented enterprise-wide schedule.
- Ambulatory appointment scheduling: e.g., for clinics, exam rooms, procedure rooms.
- Surgery scheduling: inpatient or outpatient [3.50].

(18E) Projections
This message/communications EC specifies interchange of information sufficient to enable critical operational projections, on a prospective basis.
Examples:
- Cost projections
- Resource projections: facilities, locations, staff, time, equipment, supplies

19. Work Flow

(19A) Work Flow
This message/communications EC specifies interchange of information sufficient to enable and track operational work flow.
Example:
- Real-time, work flow engine integrated across a healthcare provider organization, an integrated delivery network.

(19B) Continuity, Completeness
This message/communications EC specifies interchange of information sufficient to ensure the continuity and completeness of work flow and the corresponding healthcare delivery process.
Examples:
- Work flow, healthcare delivery process completion summary:
  - What's incomplete?
  - Where are the gaps?
  - Who's responsible?

20. Concurrent Status, Records

(20A) Concurrent Subject of Care Status
This message/communications EC specifies interchange of information sufficient to concurrently track subject of care health status and related healthcare delivery services.
Example:
- Real-time, subject of care-centered status tracking: e.g.,
  - Current health status
  - Current problems, symptoms, diagnoses
  - Personal schedule of forthcoming events
  - Events in progress, current status
  - Current problem-oriented episodes, active problem list, milestones, status
  - Current protocols (e.g., care plans, critical paths): status, milestones, variances
  - Current encounters, visits
  - Current medications
  - Current diagnostics, results
  - Currently assigned healthcare professionals, caregivers

(20B) Concurrent Practitioner Status
This message/communications EC specifies interchange of information sufficient to concurrently track healthcare professional status and related healthcare delivery services.

- Real-time, healthcare professional-centered tracking of assigned responsibilities and incomplete work list.

21. Retrospective Status, Records

(21A) Retrospective Status, Records
This message/communications EC specifies interchange of information sufficient to retrospectively track health status and healthcare delivery services.
Example:
- Real-time, subject of care-centered history:
  - Previous health status
  - Previous problems, symptoms, diagnoses
  - Events complete, in terminus status
  - Previous problem-oriented episodes
  - Previous protocols (e.g., care plans, critical paths): milestones, variances
  - Previous encounters, visits
  - Previous medications
  - Previous diagnostics, results
  - Previously assigned healthcare professionals, caregivers

22. Personal Healthcare Professional Services

(22A) Personal Healthcare Professional Portal
This message/communications EC specifies interchange of information sufficient to support a personalized healthcare professional portal.
Example:
- Personal portal to the electronic health record for a healthcare provider organization, for an integrated delivery network.

(22B) Personalized Functions
This message/communications EC specifies interchange of information sufficient to enable functions personalized to individual healthcare professionals, caregivers.
Example:
- Based a practitioner's own criteria, personal:
  - Views of the health record and its subsets
  - Orders, order sets
  - Protocols
  - Decision support, decision agents

23. Data Integrity

(23A) Data Integrity
This message/communications EC specifies interchange of information sufficient to ensure data integrity.
Examples:
- Assurance of uniform data definition.
- Assurance of uniform data context, comparability.
- Assurance of uniform vocabulary, coding and classification.
- Assurance of data integrity in the course of interchange from point of origin (point of service/care) to point of use.

24. Protocols: Care Plans, Critical Paths

(24A) Protocol Basis
This message/communications EC specifies interchange of information sufficient to enable protocol customisation

Examples:
- Standard clinical protocols from recognized authorities: e.g., professional societies.
- Protocols defined for particular diagnoses, disease states.
- Protocols defined for organizations, business units: e.g., department, services, specialties.
- Protocols defined for individual healthcare professionals or groups.

(24B) Protocol Management
This message/communications EC specifies interchange of information sufficient to enable real-time protocol management.
Examples:
- Real-time highly integrated protocol management engine for subjects of care served by a healthcare provider organization, by an integrated delivery network.
- Immediate, interactive review of protocol status: by individual subject of care, health plan member.
- Real-time protocol variance monitor.
- Protocol override, variance authorization.

25. Problem Lists

(25A) Problem List Management
This message/communications EC specifies interchange of information sufficient to enable real-time problem list management.
Examples:
- Real-time highly-integrated problem list manager for subjects of care served by a healthcare provider organization, by an integrated delivery network.
- Immediate, interactive review of current problem list: by individual subject of care, health plan member.
- Current problem definition, status, milestones.
- Current problem in terms of corresponding protocols: care plans, critical paths.
- Current problem in terms of assigned responsibilities.
- Review of previous problems: problem, milestones, final resolution/status.

26. Decision Support[3.22]

(26A) Decision Support Services
This message/communications EC specifies interchange of information sufficient to enable decision support.
Examples:
- Real-time decision agents interactive at the point of service/care.
- Background decision agents scanning for particular conditions and initiating relevant notifications.

27. Surveillance, Metrics and Analysis

(27A) Measures and Indicators
This message/communications EC specifies interchange of information sufficient to enable definitions, rules, measures and indicators with regard to key aspects of clinical and operational performance and quality.
- Examples:
- Definitions, rules, measures and indicators for clinical aspects, including:
  - Continuity, completeness: of the healthcare or operations record, of work flow and the health delivery process
  - Compliance: e.g., with standards of practice/care
  - Performance, effectiveness
  - Quality
  - Outcomes
  - Protocols, variances

- Definitions, rules and measures and indicators for operational aspects, including:
  - Allocation, deployment
  - Assigned responsibility
  - Resource utilization: facilities, locations, staff, time, equipment, supplies
  - Costs
  - Productivity, workload

(27B) Epidemiological Surveillance
This message/communications EC specifies interchange of information sufficient to enable epidemiological surveillance.

28. Communications Infrastructure

(28A) Communications Infrastructure
This message/communications EC specifies interchange of information sufficient to ensure timely and reliable information conveyance.
Example:
- Optimised communications infrastructure for a healthcare provider organization and its business units or an integrated delivery network.

29. Multiple Person Linkage [3.43]

(29A) Multiple Person Linkage
This message/communications EC specifies interchange of information sufficient to enable the logical linkage of multiple persons.
Examples of logical person linkages:
- Next of kin, family members
- Mother/child
- Multiple birth, including sequence
- Payment guarantor, guarantee
- Insured, subscriber, health plan member
- Emergency contact(s)

30. Subject of Care - Practitioner Linkage

(30A) Practitioner, Subject of Care Linkage
This message/communications EC specifies interchange of information sufficient to enable the logical linkage of subjects of care and healthcare professionals.
Example:
- Assured linkage of healthcare professionals with assigned responsibility for a given subject of care.

31. Localization, Local Authority

(31A) Localization
This message/communications EC specifies interchange of information sufficient to enable localization.
Examples:
- Local business and clinical practice rules.
- Local language, vocabulary, code sets.
- Local adaptation per business unit, organization or integrated delivery network.

32. User Environments

(32A) User Environments
This message/communications EC specifies interchange of information sufficient to support discrete

Examples:
- Production
- Test, development
- Education, training

33. Version Management

(33A) Version Management
This message/communications EC specifies interchange of information sufficient to enable version management and rollover to new revisions.
Examples of versioned constructs:
- Application, component or device software.
- Vocabulary: code sets, classification schemes.
- Master definition files.
- API standards.
- Message, EDI standards: i.e., ISO OSI Level 7 (HL7, EDIFACT).
- Network, communications standards: i.e., ISO OSI Levels 1-6.

34. Inter-Application

Examples:
- API based applications and components conjoined in a tightly coupled manner to support a healthcare provider organization or integrated delivery network.
- Interconnected applications and components joined in a loosely coupled message-based interface scheme.

(34A) Application Roles
This message/communications EC specifies interchange of information sufficient to enable specific application/component roles, as explicitly described.

(34B) Application Interactions
This message/communications EC specifies interchange of information sufficient to support typical application/component interaction paradigms.

(34C) Inter-Application Relationships
This message/communications EC specifies interchange of information sufficient to enable typical inter-application/component relationships.

(34D) Inter-Application Services
This message/communications EC specifies interchange of information sufficient to enable typical inter-application/component services.

35. Change Scale

(35A) Change scale
This message/communications EC specifies interchange of information sufficient to enable broad extensibility and change of scale of health record systems and the environments they support.
Examples:
- Change scale from small to medium to large healthcare provider organization.
- Change scale to a large integrated delivery network.
- Change scale from few to many subjects of care, health plan members.
- Change scale from few to many healthcare professionals.
- Change scale from few to many interconnected applications, components and devices.
- Change scale from encounter based health record to lifetime subject of care health record.
- Change scale from few to many transactions per unit time.

- Change scale without appreciable performance barriers.

36. Validation

(36A) Validation

This message/communications EC has evidenced substantial, broad-based validation in the environments to which it is targeted and in terms of the purposes for which it is intended.
Examples:

- Validation in number of vendor products supporting production implementations.
- Validation in number of discrete sites implemented.
- Validation in diversity and scale of implementations.

Part II: Essential Attributes

The following sections are a listing of the Essential Attributes proposed as those that underpin the listed Essential Characteristics for a messaging and communications standard. Each Attribute is numbered to aid cross-referencing with the Essential Characteristics listed in Part I.

1. Identifiable Information

(1A) Interchange of Identifiable Information
Identifiable parties (may) include:

- As subjects of the health record, e.g.:
  - Individual subjects of care;
  - Individual healthcare professionals/caregivers;
  - Individual originators of record content: authors, scribes and verifiers;
  - Organizations, including: providers, health plans;
  - Business units, including: departments, services, specialties;
  - Others, including: next of kin, emergency contacts, payment guarantors;
- As parties participating in the provision, performance and completion of healthcare services and whose related actions are ascribed in the health record, e.g.:
  - Individual healthcare professionals/caregivers;
  - Organizations;
  - Business units;
- As parties participating in the origin, amendment, stewardship and use of the health record and whose related actions are ascribed therein, e.g.:
  - Individual healthcare professionals/caregivers;
  - Individual authors, scribes and verifiers;
  - Organizations;
  - Business units.

2. Architectural Basis

(2A) Architectural Basis
Architectural constructs (may) include the following details:

- Data Definition
  - Health record and its subsets
  - Data groups: datasets, templates
  - Attributes: data elements
  - Identifiers
  - Business objects, relationships
- Information Model
  - Business classes (objects)
  - Subject areas
  - Subject classes (i.e., stateful classes)
  - Attributes, identifiers
  - Relationships between classes, attributes
  - Vocabulary, coding, classification
  - Audit
- Business Operations (Process) Model
  - Actors (including accountable parties/agents)
  - Actions (including accountable actions)
  - States, state/transitions
  - Work flow
  - Audit
- Information Flow Model
  - End-to-end
  - Point of origination (point of service/care) to point of use

- Front-end to back-end to third party
- Stewardship, chain of custody
- Audit

♦ Application Interoperability Model
For applications or software components:
- Application role(s)
- Application interactions: as sender, as receiver
- Trigger events
- Unsolicited updates
- Query/response
- Receipt acknowledgment
- Inter-application relationships
- Point to point interaction model: paired sender/receiver
- Inter-dependencies
- Application binding
- API: tightly coupled, passed parameters
- Message: loosely coupled (e.g., EDI/EDIFACT, HL7, DICOM, MIB)
- Mediated interchange (e.g., via interface engines, hubs)
- En-route queuing, store and forward
- En-route translation, transformation: of data groups, of attributes
- Acknowledgment
- Security, access control
- Audit
- Clock synchrony
- Data synchrony
- Transactions, multi-phase commits (to synchronous data stores)
- Data definition
- Master files
- Master registries

♦ Security, Access Control Model
- Access control
- Classifications: information, function
- Clearances: users, roles
- Security policy domains
- Authentication: user, data source, data verification, transmittal, receipt
- Non-repudiation
- Digital signature
- Audit

♦ Accountability Model (integral to the Security, Access Control Model)
- Accountable parties/agents
- Accountable actions

♦ Vocabulary Model
- Vocabulary domains
- Coding, classification schemes

3. Master Files

(3A) Master Files – In General
For such interchange, messages (may) include:

♦ Synchronize, across 2-n master files:
- at initial application binding
- dynamic, in real-time
- individual definition instance
- 2-n definition instances
- all definition instances

- Find/match definition instance, using matching identifier(s) and/or trait(s)
- Update definition instance, including identifier(s) and/or trait(s) and including actions to: originate, amend/translate
- Verify definition instance
- Activate/deactivate definition instance
- List audit trail for definition instance
- Update audit trail for definition instance, including actions to: access, originate, amend/translate, verify, transmit, receive
- Enable master file transaction, multi-phase commit: bid, open/lock, update, close/unlock
- Archive definition record(s).

(3B) Master File: Data Definition

Data definitions (may) include:

- Health records and subsets thereof:
  - personal health record: for individual subject of care, health plan member
  - population health record
  - business (operations) record: for organizations, business units
  - personal service record: for individual healthcare professional, caregiver
- Data groups (data sets, templates)
  - naming, identifier(s)
  - precise usage
  - aggregated attributes (contained therein)
  - at the data group level, measures and rules for: accuracy, context, consistency, comparability, continuity, completeness, relevance
- Attributes (data elements)
  - naming, identifier(s)
  - precise usage
  - data type, format
  - classification, coding scheme[3.17]
  - range
  - at the attribute level, measures and rules for: contextual data (attribute) relationships,
  - consistency, comparability, continuity, completeness, relevance
- Business Classes (Objects)
  - naming, identifier(s)
  - precise usage
  - relationships with other business objects
  - aggregated attributes (contained therein)
  - at the class level, measures and rules for: accuracy, context, consistency, comparability, continuity, completeness, relevance.

(3C) Master File: Context Sets/Templates

Context set definitions (may) include:

- Accountability [3.2] Context
- Data Integrity Context
- Clinical Context
- Operational Context

(3D) Master File: Function Definition

Function definitions (may) include:

- Information access, management and processing functions.

(3E) Master File: Security Classification Definition

Security classification definitions (may) include:

- Classification of information, for aggregations or units of information: e.g.,
  - health records and subsets thereof;
  - data groups (datasets);

- attributes (data elements);

- Access permissions for information: e.g., access/use, originate, amend/translate, verify, duplicate, disclose, transmit, receive;
- Classification of functions: e.g., for information access, management and processing functions, for firewalls [3.30] installed;
- Access permissions for functions: e.g., access, process.

(3F) Master File: Security Clearance Definition
Security clearance definitions (may) include:
- Clearances for accountable healthcare parties: individuals, organizations, business units.
- Clearances for accountable healthcare roles.

(3G) Master File: Security Policy Domain Definition
A security policy domain enables a discrete set of:
- Security classifications: for information and functions;
- Security clearances: for accountable healthcare parties and roles.

(3H) Master File: Orders, Order sets
[…]

(3I) Master File: Services, Service Events
[…]

(3J) Master File: Work Flow
[…]

(3K) Master File: Protocols (Care Plans, Critical Paths)
[…]

(3L) Master File: Decision Support Rules, Conditions, Actions
[…]

(3M) Master File: Facilities, Locations
[…]

(3N) Master File: Resources
[…]

(3O) Master File: Charges, Costs
[…]

4. Master Registries

(4A) Master Registry: Accountable Healthcare Parties
For the interchange of registry information, messages (may) include:
- Synchronize, across 2-n registries:
  - at initial application binding
  - dynamic, in real-time
  - individual party instance
  - 2-n party instances
  - all party instances in registry
- Find/match party instance, using identifier(s) and/or trait(s).
- Update party instance, its identifier(s) and/or trait(s), including actions to: originate, amend/translate.
- Verify party instance.
- Activate/deactivate party instance.
- Enable/disable party's security clearances: for access to information, to functions.

- Merge/unmerge party instances.
- List audit trail for party instance.
- Update audit trail for party instance, including actions to: access, originate, amend/translate, verify, activate/deactivate, enable/disable security clearances, merge/unmerge, transmit, receive.
- Enable transaction, multi-phase commit: bid, open/lock, update, close/unlock.
- Archive party instance.

(4B) Master Registry: Accountable Healthcare Roles

For the interchange of registry information, messages (may) include:

- Synchronize, across 2-n registries:
  - at initial application binding
  - dynamic, in real-time
  - individual role instance
  - 2-n role instances
  - all role instances in registry
- Find/match role instance, using identifier(s) and/or trait(s).
- Update role instance, its identifier(s) and/or trait(s), including actions to: originate, amend/translate.
- Verify role instance.
- Activate/deactivate role instance.
- Enable/disable role's security clearances, for access to information, to functions.
- Merge/unmerge role instances.
- List audit trail for role instance.
- Update audit trail for role instance, including actions to: access, originate, amend/translate, verify, activate/deactivate, enable/disable security clearances, merge/unmerge, transmit, receive.
- Enable transaction, multi-phase commit: bid, open/lock, update, close/unlock.
- Archive role instance.

(4C) Master Registry: Accountable Healthcare Agents [See Section 7 above.]

For the interchange of registry information, messages (may) include:

- Synchronize, across 2-n registries:
  - at initial application binding
  - dynamic, in real-time
  - individual agent instance
  - 2-n agent instances
  - all agent instances in registry
- Find/match agent instance, using identifier(s) and/or trait(s).
- Update agent instance, its identifier(s) and/or trait(s), including actions to: originate, amend/translate.
- Verify agent instance.
- Activate/deactivate agent instance.
- List audit trail for agent instance.
- Update audit trail for party instance, including actions to: access, originate, amend/translate, verify, activate/deactivate, transmit, receive.
- Enable transaction, multi-phase commit: bid, open/lock, update, close/unlock.
- Archive agent instance.

(4D) Master Registry: Persons (Health Subjects)

For the interchange of registry information, messages (may) include:

- Synchronize, across 2-n registries:
  - at initial application binding
  - dynamic, in real-time
  - individual person instance
  - 2-n person instances
  - all person instances in registry
- Find/match person instance, using identifier(s) and/or trait(s).

- Update person instance, its identifier(s) and/or trait(s), including actions to: originate, amend/translate.
- Verify person instance.
- Merge/unmerge person instances.
- Link/unlink person instance to encounter.
- List audit trail for person instance.
- Update audit trail for person instance, including actions to: access, originate, amend/translate, verify, merge/unmerge, link/unlink encounters, transmit, receive.
- Enable transaction, multi-phase commit: bid, open/lock, update, close/unlock.
- Archive person instance.

(4E) Local Identifier Assignment

5. Electronic Records

(5A) Personal Health Record

For the interchange of personal health record(s), messages (may) include:

- Synchronize, across 2-n health record systems:
  - at initial application binding
  - dynamic, in real-time
  - personal health record
  - 2-n personal health records
  - all personal health records
- Update audit trails for personal health record interchange: access, amend/translate, transmit, receive.
- Enable interchange based on security classifications, security clearances and data definitions.
- Enable transaction, multi-phase commit: bid, open/lock, update, close/unlock.
- Archive personal health record.

(5B) Population Health Record

For the interchange of population health record(s), messages (may) include:

- Synchronize, population health record, across 2-n health record systems:
  - at initial application binding
  - dynamic, in real-time
- Update audit trails for population health record interchange: access, amend/translate, transmit, receive.
- Enable interchange based on security classifications, security clearances and data definitions.
- Enable transaction, multi-phase commit: bid, open/lock, update, close/unlock.
- Archive population health record.

(5C) Business (Operations) Record

For the interchange of business record(s), messages (may) include:

- Synchronize business record, across 2-n record systems.
  - at initial application binding
  - dynamic, in real-time
- Update audit trails for business record interchange: access, amend/translate, transmit, receive.
- Enable interchange based on security classifications, security clearances and data definitions.
- Enable transaction, multi-phase commit: bid, open/lock, update, close/unlock.
- Archive health records

(5D) Personal Practitioner Service Record

For the interchange of personal service record(s), messages (may) include:

- Synchronize business record, across 2-n record systems.
  - at initial application binding
  - dynamic, in real-time
- Update audit trails for business record interchange: access, amend/translate, transmit, receive.

- Enable interchange based on security classifications, security clearances and data definitions.
- Enable transaction, multi-phase commit: bid, open/lock, update, close/unlock.
- Archive personal service record(s).

(5E) Multi-Media Record
Multi-media formats (may) include:
- Text
- Audio
- Video
- Image, graphic
- Waveform
- Binary

6. Record Chronology, Continuity, Completeness

(6A) Chronological Order of Events

(6B) Event Timeline

(6C) Historical Snapshot

(6D) Continuity, Completeness
Relevant functions may include:
- Completeness metrics: for the health record and its subsets, for data groups (i.e., data sets), attributes (i.e., data elements)
- Gap analysis

7. Authentication, Non-Repudiation Services

(7A) User Authentication.

(7B) Data Source Authentication

(7C) Validation Authentication.

(7D) Data Interchange Authentication

(7E) Non-Repudiation Services

8. Digital Signature

(8A) Digital Signature

(8B) Public/Private Key Infrastructure (PKI)

9. Audit

(9A) Audit Trails
Audit trails (may) track:
- Provision, performance and/or completion of healthcare services, and specifically health service events: as healthcare professionals and caregivers.
- Access to, and use of, record content.
- Escrow agreement provided and sealed
- Origin or amendment of record content: as authors, scribes.
- Verification of record content.
- Duplication of record content.
- Disclosure, transmission or receipt of record content

- Translation of record content.

(9B) Audit Review

10. Permanence, Persistence, Non-Alterability

(10A) Permanence, Persistence, Non-Alterability
Relevant functions (may) include:
- Preservation of the record and its subsets, data groups and attributes
- Escrow agreement provided and sealed
- Non-alterability of content
- Formal amendment process, preserving previous content
- Data state preservation: initial and through each amendment

11. On-Line Transaction Processing (OLTP)

(11A) Tightly Coupled OLTP Services

(11B) Multi-Phase Commit

12. On-Line Analytical Processing (OLAP)

(12A) OLAP

13. Fault Tolerance

(13A) Redundant Communications Architecture

(13B) Unavailability/Failure Detection

(13C) Availability/Restart Detection

(13D) Downtime and Slow Response Queuing

(13E) Recovery

14. Data Synchrony

(14A) Data Synchronization

15. Time Synchrony

(15A) Time Synchrony

16. Trusted End-to-End Information Flows

(16A) Trusted End-to-End Information Flows

(16B End-to-End Record Audit
Major audits (may) include:
- Provision, performance and/or completion a health service event (often the sentinel trigger event from which information flows)
- Access to, and use of, the record or information
- Firewall installation
- Origination or amendment of the record or information
- Verification of record or information
- Duplication of record or information

- Disclosure, transmission or receipt of record or information
- Translation of record or information
- Stewardship of record or information (i.e., data at rest)

(16C) Chain of Custody Audit

(16D Context Sets, Templates

17. Disclosure, Export

(17A) Disclosure Authorization, Scope
Authorization functions (may) include:
- Subject of care authorization for release of information
  - Scope of information eligible for disclosure
  - To whom
  - For what purpose
  - For what duration

(17B) Controlled Disclosure Tracking
Services (may) include:
- Disclosure, transmittal audits
- Receipt audits

(17C) Disclosure Labelling

(17D) Remove identification, Aliasing
Related services (may) include purging or aliasing of:
- Identifiers for individuals, organizations, business units
- Personal demographics and traits
- Sensitive/protected information related to
  - Individual subjects of care, health plan members
  - Individual healthcare professionals, caregivers
  - Organizations, business units

18. Prospective Services

(18A) Subject of Care Schedule
Schedule features (may) include:
- Integrated schedule across multiple care disciplines, business units: departments, services, specialties
- Integrated schedule encompassing all venues and encounter types: inpatient [3.39], emergent, ambulatory, long-term care, home care
- Timeline based, including forthcoming clinical service events
- Wellness and follow-up events
- Initiated by healthcare professional orders, order sets
- Initiated by protocols: care plans, critical paths
- Medication profile, medication events

(18B) Assigned Responsibility
Assignment features (may) include:
- Assignments to specific individual healthcare professional
- Assignments to a healthcare group
- Assignments to a healthcare role

(18C) Healthcare Professional Schedule
Schedule features (may) include:

- Assigned responsibility
- Business and clinical rules based

(18D) Resource Schedule

Schedule features (may) include:

- Business and clinical rules based
- Resource factors:
  - Facilities, locations
  - Staff resource factors
  - Time resource factors
  - Equipment resource factors
  - Supply resource factors
- Review options:
  - By individual subject of care
  - By individual healthcare professional
  - By healthcare group or role
  - Across/by organization or business unit: department, service, specialty
  - By resource: facility, location, equipment

(18E) Projections

Services (may) include:

- Optimal allocations, deployments
- Business and clinical rule based

19. Work Flow

Work Flow

(19A) Work Flow

Work flow features (may) include:

- Real-time, interactive work flow management
- Shared work flow management
  - Among associated healthcare professionals, groups
  - Across and among disciplines, business units
  - Across multiple venues and encounter types: inpatient, emergent, ambulatory, long term care, home care
- Based on tight integration of prospective schedules: subject of care, healthcare professional, resource
- Allocation, deployment of critical resources: facilities, locations, staff time, equipment, supplies, etc.
- Work flow services
  - Initiate, assign
  - Allocate, deploy (resources)
  - Condition
  - Stage, sequence, route
  - Track, checkpoint, status
  - Complete
- Initiation
  - By orders, order sets
  - By protocols: care plans, critical paths
- Threading
  - Single-threaded work flow: tasks in sequence
  - Multi-threaded work flow: tasks in parallel
- Inter-dependencies: tightly coupled tasks

- Based on business and clinical practice rules

(19B) Continuity, Completeness

Services (may) include:
- Completeness metrics
- Continuity monitors, from initiation through completion
- Gap analysis

20. Concurrent Status, Records

(20A) Concurrent Subject of Care Status

(20B) Concurrent Healthcare Professional Status

21. Retrospective Status, Records

(21A) Retrospective Subject of Care Record

22. Personal Healthcare Professional Services

(22A) Personal Healthcare Professional Portal
Personal practitioner portal services (may) include:
- Assigned responsibilities, incomplete work list: personal or for affiliated healthcare group
- Action items (e.g., items requiring signature)
- Notifications, prompts, alerts, reminders
- E-mail functions
- Significant, un reviewed events since last access (e.g., new critical results)
- Based on personalized criteria

(22B) Personalized Functions

23. Data Integrity

(23A) Data Integrity
Data integrity services (may) include:
- Uniform data definition, at various levels of data granularity
  - Public data registry (e.g., USHIK)
  - Health record and its subsets
  - Data groups (i.e., data sets)
  - Attributes (i.e., data elements)
- Measures and indicators for accuracy, context, consistency, comparability, continuity, completeness, relevance
- Systematic, uniform data capture
- Consistent, structured content
- Consistent vocabulary, coding and classification

24. Protocols: Care Plans, Critical Paths

(24A) Protocol Basis

(24B) Protocol Management

25. Problem Lists

(25A) Problem List Management

26. Decision Support

(26A) Decision Support Services
Services (may) include:
- Based on:
  - Business and clinical practice rules
  - Practice guidelines, standards of care
  - Protocols
  - Performance measures
  - Outcome indicators
  - Cost parameters
- Detection of:
  - Duplicate/redundant clinical services
  - Conflicts and interactions
- Real-time, concurrent decision support
  - At the point of service/care
  - At the point of completion of clinical service events: e.g., results, interventions, observations
- Retrospective decision support: e.g., data warehousing
- Condition predicated actions, to:
  - Initiate notifications, prompts, alerts, reminders
  - Initiate orders, order sets
  - Initiate, revise protocols
  - Initiate, cancel, hold clinical service events
- Link decision support based actions into health record

27. Surveillance, Metrics and Analysis

(27A) Measures and Indicators

(27B) Epidemiological Surveillance

28. Communications Infrastructure

(28A) Communications Infrastructure
Services (may) include:
- Real-time, immediate information conveyance: e.g., point of origination (point of service/care) to point of use
- Notifications, prompts, alerts, reminders
- E-mail functions
- Telephone replacement functions
- Paper replacement functions
- Affirmative acknowledgement of receipt: by individual healthcare professionals, caregivers

29. Multiple Person Linkage

(29A) Multiple Person Linkage

30. Subject of Care – Healthcare Professional Linkage

(30A) Healthcare Professional, Subject of Care Linkage

31. Localization, Local Authority

(31A) Localization
Localization (may) include:
- Security, access control:

- Security policies, policy domains
- Classifications: functions, information
- Clearances: users, roles

- Identifiers
- Accountable healthcare parties, agents
- Accountable healthcare roles
- Accountable healthcare groups
- Data definitions: health record and its subsets, data groups, attributes
- Context sets, templates
- Business and clinical practice rules
- Practice guidelines, standards of care
- Orders, order sets
- Services, service events
- Work flow
- Protocols: care plans, critical paths
- Decision support rules, conditions, actions
- Facilities, locations
- Charges, costs
- Surveillance, metrics and analysis: rules, measures and indicators etc.

32. User Environments

(32A) User Environments

33. Version Management

(33A) Version Management

34. Inter-Application

(34A) Application Roles

(34B) Application Interactions
Relevant paradigms (may) include:
- Trigger events
- Unsolicited updates
- Query/response
- Receipt acknowledgement

(34C) Inter-Application Relationships
Relevant relationships (may) include:
- Point to point interaction model: paired sender/receiver
- Inter-dependencies

(34D) Inter-Application Services
Services (may) include:
- API: tightly coupled, passed parameters
- Message: loosely coupled (e.g., EDI/EDIFACT[3.25], HL7, DICOM, MIB)
- Mediated message interchange (e.g., via interface engines, hubs)
  - En-route queuing, store and forward
  - En-route translation, transformation: of data groups, of attributes
  - Phase I acknowledgement: mediator to transmitter
  - Phase II acknowledgement: receiver to mediator
  - End-to-end acknowledgement: receiver to transmitter
  - Phase I threaded message sequence: transmitter to mediator
  - Phase II threaded message sequence: mediator to receiver

- End-to-end threaded message sequence: transmitter to receiver

- Security, access control
- Audit
- Clock synchrony
- Data synchrony
- Transactions, multi-phase commits (to synchronous data stores)
- Data definition
- Master files
- Master registries

35. Change Scale

(35A) Change Scale

36. Validation

(36A) Validation

Table 3: Principles and Objectives Linked to Essential Characteristics

PRINCIPLES AND OBJECTIVES	ESSENTIAL CHARACTERISTICS	DETAIL NUMBERED
1. Ensured Trust	Identifiable Information	1A
	Architectural Basis	2A
	Master Files	3 D 3E 3F 3G
	Master Registries	4A
	Electronic Records	5A
	Authentication Non-repudiation services	7A 7B 7C 7D 7E
	Digital signature	8A 8B
	Permanence Persistence Non-alterability	10A
	On-Line Transaction Processing	11A 11B
	Trusted End-to-End information Flows	16A 16B 16C
	Disclosure, Export	17A 17B 17D
	Concurrent Status, Records	20A
	Retrospective Status, Records	21A
	Data Integrity	23A
	Problem Lists	25A
	Surveillance, Metrics and Analysis	27A 27B
	Communications Infrastructure	28A
	Subject of Care-Practitioner Linkage	30A
	User Environments	32A
	Validation	36A
2. Trust Constituency	Identifiable Information	1A
	Architectural Basis	2A
	Master Files	3B 3D
	Master Registries	4A 4B 4C 4D
	Electronic Records	5A 5C 5D 5E
	Record Chronology, Continuity, Completeness	6D
	Permanence Persistence Non-alterability	10A
	Prospective Services	18A 18B 18C 18D
	Concurrent Status, Records	20A 20B
	Retrospective Status, Records	21A
	Personal Practitioner Services	22A 22B
	Data Integrity	23A
	Surveillance, Metrics and Analysis	27A 27B
	Communications Infrastructure	28A
	Subject of Care – Practitioner Linkage	30A
	Validation	36A
3. Health Record Rights	Identifiable Information	1A
	Master Files	3A 3B 3E 3F 3G
	Master Registries	4A 4B 4C 4D
	Electronic Records	5A 5B 5C 5D 5E
	Record chronology, Continuity, Completeness	6A 6B 6C 6D
	Authentication non-repudiation Services	7A 7B 7C 7D 7E
	Permanence Persistence Non-alterability	10A
	Trusted End-to-End Information Flows	16A 16B 16C
	Disclosure, Export	17A 17B
	Concurrent Status, Records	20A 20B
	Retrospective Status, Records	21A
	Personal Practitioner Services	22A 22B
	Data Integrity	23A
	Communications Infrastructure	28A
	Multiple Person Linkage	29A
	Subject of Care – Practitioner Linkage	30A
	Validation	36A

4. Health Record Obligations	Identifiable Information Architectural Basis Master Files Master Registry Electronic Record Record Chronology, Continuity, Completeness Authentication Non-repudiation services Audit Permanence Persistence Non-alterability On-line Transaction Processing On-Line Analytical Processing Disclosure, Export Concurrent Status, Records Retrospective Status Records Data Integrity Decision Support Subject of Care – Practitioner Linkage Localisation, Local Authority Validation	1A 2A 3A 3B 3D 3E 3F 3G 4A 4B 4C 4D 4E 5A 5B 5C 5D 5E 6A 6B 6C 6D 7A 7B 7C 9B 10A 11A 12A 17A 17D 20A 20B 21A 23A 26A 30A 31A 36A
5. Health Record Composition	Identifiable Information Architectural basis Master Files Master Registries Electronic Records Record Chronology, Continuity, Completeness Permanence persistence Non-alterability Concurrent Status, Records Retrospective Status, Records Personal Practitioner Services Data Integrity Subject of care-practitioner Linkage Localisation, Local authority	1A 2A 3A 3B 3C 4A 4B 4C 4D 4E 5A 5C 5E 6A 6B 6C 6D 10A 20A 20B 21A 22B 23A 30A 31A
6. Healthcare Parties and Their Accountable Actions	Identifiable Information Architectural Basis Master Files Master Registries Electronic records Record chronology, Continuity, Completeness Authentication Non-repudiation services Digital Signature Permanence persistence Non-alterability On-Line Transaction Processing On-Line Analytical Processing Trusted End-to-End Information Flows Prospective Services Work Flow Concurrent Status Retrospective Status, Records Personal Practitioner Services Data Integrity Protocols: Care Plans, Critical Paths Decision Support Surveillance, Metrics and Analysis Multiple Person Linkage Subject of Care – Practitioner Linkage Localisation. Local Authority User Environments Change of Scale Validation	1A 2A 3A 3B 3D 3E 3F 3G 4A 4B 4C 4D 4E 5A 5B 5C 5D 5E 6A 6B 6C 7A 7B 7C 7D 7E 8A 10A 11A 11B 12A 16A 18A 18B 18C 18D 18F 19A 19B 20A 20B 21A 22A 22B 23A 24A 24B 26A 27A 27B 29A 30A 31A 32A 35A 36A

7. Healthcare Agents and Their Accountable Actions	Identifiable information Architectural Basis Master Files Authentication Non-repudiation services On-Line transaction Processing Trusted End-to-End Information Flows Data Integrity Surveillance, Metrics and Analysis Communications Infrastructure Localisation, Local Authority User Environments Inter-Application	1A 2A 3A 3C 3D 7A 7B 7D 11A 11B 16A 16C 23A 27A 27B 28A 31A 32A 34A 34B 34C 34D
8. Scope of Accountability, Unit of Accountability	Electronic records Audit Permanence persistence Non-alterability Prospective Services Work flow Concurrent Status, Records Retrospective Status, Records Personal practitioner services Data Integrity Decision support Surveillance, metrics and Analysis Subject of Care-Practitioner Linkage Localisation, Local Authority User Environments Change of Scale	5A 5B 5C 5D 5E 9A 9B 10A 18A 18B 18C 18D 18E 19A 19B 20B 21A 22A 22B 23A 26A 27A 27B 30A 31A 32A 35A
9. Authentication, Attestation, Non-repudiation, Digital Signature	Electronic records Record Chronology, Continuity, Completeness Authentication Non-repudiation services Digital Signature Permanence Persistence Non-alterability Fault Tolerance Trusted End-to-End Information Flows Disclosure, Export Concurrent status, Records Retrospective Status, Records Data Integrity Problem Lists Subject of Care – Practitioner Linkage Version Management Validation	5A 6A 6C 6D 7A 7B 7C 7D 7E 8A 8B 10A 13A 13B 13C 13E 16B 16C 17A 17B 20A 20B 21A 23A 25A 30A 33A 36A
10. Auditability	Identifiable Information Master Files Master Registry Electronic Records Record Chronology, Continuity, Completeness Authentication Non-repudiation services Digital Signature Audit Permanence persistence Non-alterability On-Line Transaction Processing On-Line Analytical Processing Trusted End-to-End Information Flows Disclosure, Export Concurrent Status, Records Retrospective Status, Records Data Integrity Problem Lists Surveillance, Metrics and Analysis Subject of care – practitioner Linkage Validation	1A 3A 3B 3D 3E 3F 3G 4A 5A 5C 5D 5E 6A 6B 6C 6D 7A 7B 7C 7D 7E 8A 8B 9A 9B 10A 11A 11B 12A 16A 16B 16C 17A 17B 17C 17D 20A 20B 21A 23A 25A 27A 27B 30A 36A

11. Chain of Custody	Identifiable Information Architectural basis Master Files Electronic Records Authentication Non-repudiation services Digital Signature Audit Permanence persistence Non-alterability Trusted End-to-End Information Flows Disclosure, Export Concurrent Status, Records Retrospective Status, Records Data integrity Surveillance, Metrics and Analysis Communications Infrastructure Subject of Care – Practitioner Linkage Inter-Application Validation	1A 2A 3A 5A 7A 7B 7C 7D 8A 9A 9B 10A 16A 16B 16C 17A 17B 17C 20A 21A 23A 27A 28A 30A 34A 34C 36A
12. Faithfulness, Permanence, and Indelibility	Permanence, Persistence, Non-Alterability Identifiable Information Master Files Master Registries Record Chronology, Continuity, Completeness Authentication, Non-Repudiation Services Audit Review Data Synchrony Time |Synchrony Data Integrity Validation	10A 1A 3A 4A 4B 6A 6B 6D 7A 7B 9B 14A 15A 23A 36A
13. Data Definition, Data Registry	Identifiable Information Master Files Master Registries Electronic Records Record Chronology, Continuity, Completeness Permanence persistence Non-alterability Trusted End-to-End Information flows Concurrent Status Records Retrospective status, Records Data Integrity Surveillance, Metrics and Analysis Subject of care – Practitioner Linkage Validation	1A 3B 4A 4B 4C 4D 5A 5B 5C 5D 6A 6B 6D 10A 16A 16B 20A 21A 23A 27A 30A 36A
14. Data Integrity	Identifiable Information Master Files Electronic Records Record chronology, Continuity, Completeness Authentication Non-repudiation services Digital Signature Permanence persistence Non-alterability Trusted End-to-End Information Flows On-Line Analytical Processing Trusted End-to-End Information Flows Disclosure, Export Concurrent Status, Records Retrospective status, records Data Integrity Surveillance, Metrics and Analysis Communications Infrastructure Subject of care – Practitioner Linkage Validation	1A 3A 3B 5A 5C 6A 6C 6D 7A 7B 7C 8A 10A 11A 12A 16A 16C 17A 20A 20B 21A 23A 27A 28A 30A 36A

Annex A: An Exercise to Validate the Essential Characteristics Set Out In The ISO Technical Report

Members of the ISO TC/215 Medical Devices Sub-Group based at the Heinrich-Heine-Universitat Hospital, Dusseldorf, Germany devised a flow chart of activity (Diagram 1) to illustrate the different levels of communication to be found between a Hospital Information System (Level 2) i.e. a patient Health Record Server and a Departmental Computer System (level 1) in an Intensive Care Unit (ICU) - device orientated environment. Different levels of communication are evident in many other sectors of the healthcare domain, for example, general medical practitioner clinic/hospital specialist clinic; Community pharmacy/hospital pharmacy; community nursing/ hospital nursing

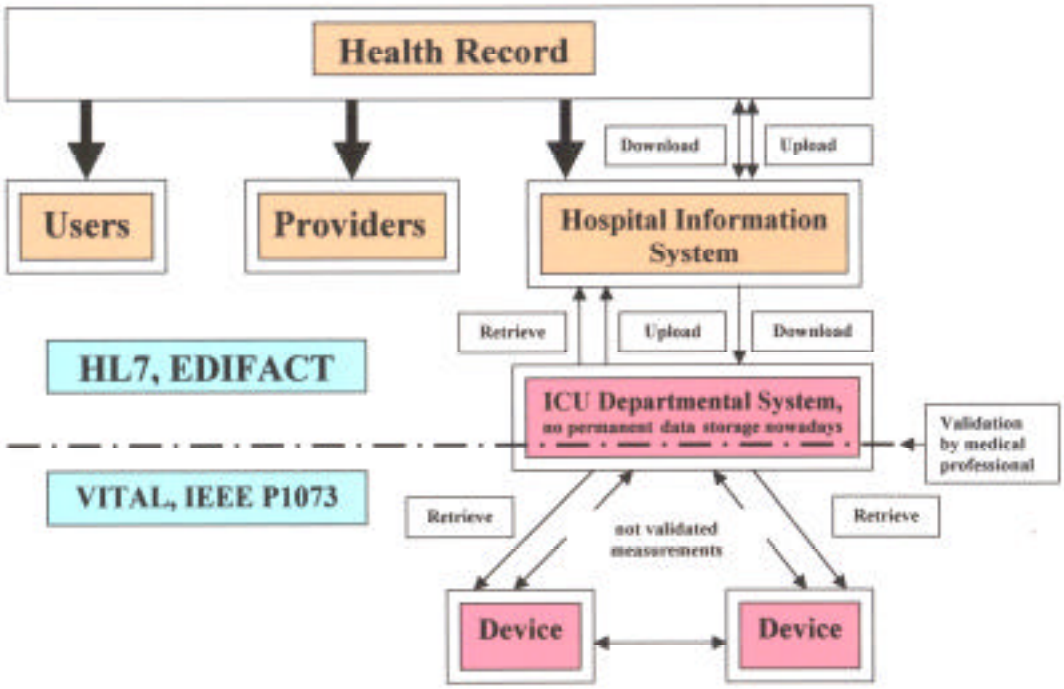

Fig. 1: Flow Chart of Communication Flows in a Hospital Environment

The Dusseldorf Team subsequently used the Essential Characteristics listed in the Technical Report to validate the recommendations in the Report. The resulting Tables demonstrate that the Essential Characteristics listed are a valuable check list of the components required to develop complete message packages.

Table 4 sets out the Critical Success Factors inherent in the design of precise healthcare electronic messages.

Table 5 addresses the applicability of the Essential Characteristics listed in the Technical Report to the ”level 1” and ”level 2” domains.

Table 4: Critical Success Factors in Message Design

Critical Success Factors:	Departmental System e.g. ICU-PDMS + Communication. => HCR	Departmental System to Device Communication
Trust: confidence, surety		
Trusted Health Record Protection and Assurance: privacy, confidentiality, stewardships, rights, obligations	yes	No
Trusted End-to-End Information Flow: point of origination (point of service/care) to point of use	NA	yes?
Security, Access Control	yes	Yes
Accountability	yes	Yes
Scope: domain	yes	Yes
Functionality	yes	Yes
Application Interoperability, Tight Coupling	yes	Yes
Suitability: fit, finish	?	?
Controllability, Adaptability, Localization	yes	Yes
Performance	yes	Yes
Data Integrity: accuracy, context, consistency, comparability, continuity, completeness, relevance	yes	Yes
Persistence, Faithfulness	yes	
Change Scale	yes	Yes
Validation	yes	Yes

Table 5: Applicability of Principles and Objectives to HIS and Departmental Systems

	Principles and Objectives	Departmental System e.g. ICU-PDMS + Communication => HCR	Departmental System to Device Communication
1.	**Ensured Trust**	yes	Yes
1.1	Privacy and confidentiality	yes	Yes
1.2	Protection of individually identifiable information	yes	Yes
1.3	Protection in the course of interchange - "in transit"	yes	Yes
2.	**Trust Constituency**	yes	NA
2.1	As subjects of the health record, e.g.:	yes	NA
2.2	As parties participating in the provision, performance and completion of healthcare services and whose related actions are ascribed	yes	NA
2.3	As parties participating in the origination, amendment, stewardship and use of the health record and whose related actions are ascribed therein, e.g.	yes	NA
3.	**Health Record Rights**	yes	NA
3.1	Confidentiality and privacy protections, particularly with regard to access to, use and disclosure of:		
3.1.1	Individually identifiable information	yes	NA
3.1.2	Information subject to protection	yes	NA
3.1.2.a	by statute, regulation, standard of practice or custom; and/or	yes	NA
3.1.2.b	by virtue of explicit disclosure grants and agreements	yes	NA
3.1.3	information made available by such grants and agreements	yes	NA
3.1.3.a	for purpose intended	yes	NA
3.1.3.b	by those parties so authorized	yes	NA
3.1.3.c	for the period (of time) designated; and	yes	NA
3.1.3.d	based on the principle of "need to know"	yes	NA
3.2	Complete and accurate portrayal of health status and intervention	yes	NA
3.3	Complete and accurate portrayal of the provision, performance and completion of health services;	Yes	NA
3.4	Detailed audit logs tracking record creation, amendment, access, use and disclosure	yes	NA
4.	**Health record obligations include accountability for:**		
4.1	record content origin and amendment, as ascribed to authors, scribes and/or verifiers;	yes	NA
4.2.	provision, performance and completion of health services, as documented in the health record and as ascribed to practitioners, caregivers;	yes	NA
4.3.	accuracy, completeness of record content;	yes	NA
4.4.	access to, and use of, record content;	yes	NA
4.5	duplication of record content;	yes?	NA

4.6.	disclosure, transmission and receipt of record content;	yes	NA
4.7.	translation of record content (e.g., to alternate coding and classification schemes).	yes	NA
5.	**Health Record Composition**		
	In its fullest instantiation, the subject of care/member health record comprises:		
5.1.	a longitudinal chronology of subject of care health status and interventions;	(yes)	NA
5.2.	a chronicle of health service events corresponding to the provision, performance and completion of health(care) services;	(yes)	NA
5.3.	a collection of discrete record instances (documents), often corresponding in a 1:1 relationship with health service events.	(yes)	NA
6.	**Healthcare Parties and Their Accountable Actions**		
	In this context, healthcare parties are those individuals, organizations and business units accountable for actions related to, and/or ascribed in, the health record, including:		
6.1.	Origin or amendment of record content: as authors, scribes, verifiers;	Yes	NA
6.2.	Provision, performance and/or completion of healthcare services, specifically health service events;	Yes	NA
6.3.	Access to, and use of, health record content;	Yes	NA
6.4.	Duplication of record content;	?	NA
6.5.	Disclosure, transmission and/or receipt of record content;	Yes	NA
6.6.	Translation of record content	?	NA
7.	**Healthcare Agents and Their Accountable Actions**		
	In this context, healthcare agents are those medical devices (e.g., instruments, monitors) and software (e.g., applications, components) accountable for actions related to, and/or ascribed in, the health record, including:		
7.1.	origin of record content (typically pre-verification);	Yes	Yes
7.2.	duplication of record content;	?	NA
7.3.	transmission and/or receipt of record content;	Yes	Yes
7.4.	translation of record content	?	NA
8.	**Scope of Accountability, Unit of Accountability**		
	Following from the above description of healthcare parties, healthcare agents and their accountable actions, it is necessary to designate a corresponding scope of accountability. Such scope includes (the domain of) health record content ascribed to:		
8.1.	healthcare parties in terms of their specific actions in the provision,	NA	NA

	performance and/or completion of health services;		
8.2	healthcare parties and agents in terms of healthcare parties and agents in terms of their specific actions in the origin, amendment, stewardship and use of the health record.	NA	NA
	The scope of accountability resolves to a discrete unit of accountability, specifically the set of attributes (data elements):		
8.3.	describing the performance, provision and/or completion of a discrete health service event;	yes?	NA
8.4.	comprising a discrete record instance.	yes?	NA
9.	**Authentication, Attestation, Non-Repudiation, Digital Signature**		
	Authentication is fundamental to trusted interchange of health information, which ensures the capability of a recipient to reliably ascertain parties to the origin, validation, transmission and receipt of health records, in whole or in part. Specific authentication functions are crucial, including:		
9.1.	user authentication: evidence of individual identity;	yes	?
9.2.	source authentication: evidence of authorship, origination, amendment;	yes	Yes
9.3.	validation authentication: evidence of data verification, e.g.:		
9.3.1	of data originated by another party;	no?	NA
9.3.2	of automated device input;	yes	NA
9.4.	data interchange authentication: evidence of transmission, receipt. Other crucial aspects of authentication include:		?
9.5.	non-repudiation (e.g., of authorship);	?	NA
9.6.	attestation;	?	?
9.7.	digital signature;	yes	NA
9.8.	public/private key infrastructure;	?	NA
9.9.	encrypted encapsulation: binding health record content to authenticated source.	?	?
10.	**Auditability**	yes	NA
11.	**Chain of Custody**	yes	NA
12.	**Faithfulness, Permanence, Persistence and Non-Alterability**		NA
	Another key requisite is the need to ensure that health records are faithfully maintained in a permanent, fully persistent, non-altered form, from point of origination to point of use. This includes:		
12.1.	preservation of original content and context;	yes	NA
12.2.	revision by (additive) amendment only;	yes	NA
12.3.	preservation of discrete data states: original and for each amendment;	yes	NA
12.4.	ability to reconstruct health records for any given historical date/time.	Yes	NA
13.	**Data Definition, Data Registry**	Yes	?
14.	**Data Integrity**	Yes	Yes

Table 6: Applicability of Essential Characteristics to HIS and Departmental Systems

	Essential Characteristics	Departmental System e.g. ICU-PDMS + Communication => HCR	Departmental System to Device Communication
1.	**Interchange of Identifiable Information**		
1.1	As subjects of the health record, e.g.:		NA
1.1.1	individual subjects of care, health plan members;	yes	yes ?
1.1.2	individual healthcare professionals/caregivers;	yes	NA
1.1.3	individual originators of record content: authors, scribes and verifiers;	yes	NA
1.1.4	organizations, including: providers, health plans;	NA?	NA
1.1.5	business units, including: departments, services, specialties;	yes	NA
1.1.6	others, including: next of kin, emergency contacts, guarantors;	yes?	NA
1.2	As parties participating in the provision, performance and completion of health(care) services and whose related actions are ascribed in the health record, e.g.:		
1.2.1	individual practitioners/caregivers;	yes	NA
1.2.2	organizations;	NA	NA
1.2.3	business units;	NA	NA
1.3	As parties participating in the origin, amendment, stewardship and use of the health record and whose related actions are ascribed therein, e.g.:		
1.3.1	individual healthcare professionals/caregivers; in this context as:	yes	NA
1.3.2	individual authors, scribes and verifiers;	yes	NA
1.3.3	organizations;	NA	NA
1.3.4	business units.	NA	NA
2.	**Architectural Basis** Architectural constructs (may) include:		
2.1	Data Definition	yes	Yes
2.1.1	Health record and its subsets	yes (subset)	(yes)
2.1.2	Data groups: datasets, templates	yes	Yes
2.1.3	Attributes: data elements	yes	Yes
2.1.4	Identifiers	yes	Yes
2.1.5	Business objects, relationships	?	?
2.2	Information Model		
2.2.1	Business classes (objects)	yes	(yes)
2.2.2	Subject areas	yes	(yes)
2.2.3	Subject classes (i.e., state-full classes)	yes	(yes)
2.2.4	Attributes, identifiers	yes	Yes
2.2.5	Relationships between classes, attributes	yes	Yes
2.2.6	Vocabulary, coding, classification	yes	Yes
2.2.7	Audit	yes?	?
2.3	Business Operations (Process) Model		
2.3.1	Actors (including accountable	yes	(Yes, devices)

	parties/agents)		
2.3.2	Actions (including accountable actions)	yes	yes?
2.3.3	States, state/transitions	yes	yes?
2.3.4	Work flow	?	?
2.3.5	Audit	?	?
2.4	Information Flow Model		
2.4.1	End-to-end	yes	yes
2.4.1.1	Point of origin (point of service/care) to point of use	yes	yes
2.4.1.2	Front-end to back-end to third party	yes	?
2.4.2	Stewardship, chain of custody	?	NA
2.4.3	Audit	?	NA
2.5	Application Interoperability Model For applications or software components:		
2.5.1	Application role(s)	yes	yes
2.5.2	Application interactions: as sender, as receiver	yes	yes
2.5.2.1	Trigger events	yes	yes
2.5.2.2	Unsolicited updates	yes	yes
2.5.2.3	Query/response	yes	yes
2.5.2.4	Receipt acknowledgment	yes	yes ?
2.5.3	Inter-application relationships	yes	?
2.5.3.1	Point to point interaction model: paired sender/receiver	?	?
2.5.3.2	Inter-dependencies	?	?
2.5.4	Application binding	?	?
2.5.4.1	API: tightly coupled, passed parameters	yes	yes
2.5.4.2	Message: loosely coupled (e.g., EDI/EDIFACT, HL7, DICOM, MIB)	yes	yes
2.5.4.3	Mediated interchange (e.g., via interface engines, hubs)	yes	yes ?
2.5.4.3.1	En-route queuing, store and forward	?	NA
2.5.4.3.2	En-route translation, transformation: of data groups, of attributes	yes	NA
2.5.4.3.3	Acknowledgment	yes	yes
2.5.4.4	Security, access control	yes	yes
2.5.4.5	Audit	?	?
2.5.4.6	Clock synchrony	yes	yes
2.5.4.7	Data synchrony	yes	yes ?
2.5.4.8	Transactions, multi-phase commits (to synchronous data stores)	yes?	?
2.5.4.9	Data definition	yes	yes
2.5.4.10	Master files	yes	????
2.5.4.11	Master registries	???	????
2.6	Security, Access Control Model		?
2.6.1	Access control	yes	?
2.6.2	Classifications: information, function	yes	?
2.6.3	Clearances: users, roles	yes	NA
2.6.4	Security policy domains	yes	NA
2.6.5	Authentication: user, data source, data verification, transmittal, receipt	yes	NA
2.6.6	Non-repudiation	?	NA
2.6.7	Digital signature	yes	NA
2.6.8	Audit	?	NA

2.7	Accountability Model (integral to the Security, Access Control Model)		
2.7.1	Accountable parties/agents	yes?	?
2.7.2	Accountable actions	yes?	?
2.8	Vocabulary Model	yes?	yes
2.8.1	Vocabulary domains	yes?	yes
2.8.2	Coding, classification schemes	yes	yes
3.	**Master Files**		
3.1	Master Files – In General		
	For such interchange, messages (may) include:		
3.1.1	Synchronize, across 2-n master files:	yes	NA
3.1.1.1	At initial application binding	yes	NA
3.1.1.2	Dynamic, in real-time	yes	NA
3.1.1.3	Individual definition instance	yes	NA
3.1.1.4	2-n definition instances	yes	NA
3.1.1.5	All definition instances	yes	NA
3.1.2	Find/match definition instance, using matching identifier(s) and/or trait(s)	yes	NA
3.1.3	Update definition instance, including identifier(s) and/or trait(s) and including actions to: originate, amend/translate	yes	NA
3.1.4	Verify definition instance	yes	NA
3.1.5	Activate/deactivate definition instance	yes	NA
3.1.6	List audit trail for definition instance	yes	NA
3.1.7	Update audit trail for definition instance, including actions to: access, originate, amend/translate, verify, transmit, receive	?	NA
3.1.8	Enable master file transaction, multi-phase commit: bid, open/lock, update, close/unlock	yes	NA
3.2	Master File: Data Definition		????
3.2.1	Health records and subsets thereof:	yes	
3.2.1.1	Personal health record: for individual subject of care health plan member	yes	NA
3.2.1.2	Population health record	NA	NA
3.2.1.3	Business (operations) record: for organizations, business units	NA	NA
3.2.1.4	Personal service record: for individual healthcare professional, caregiver	yes	NA
3.2.2	Data groups (datasets, templates)	yes	?
3.2.2.1	Naming, identifier(s)	yes	yes
3.2.2.2	Precise usage	yes	yes
3.2.2.3	Aggregated attributes (contained therein)	yes	yes
3.2.2.4	At the data group level, measures and rules for: accuracy, context, consistency, comparability, continuity, completeness, relevance	yes?	NA
3.2.3	Attributes (data elements)	yes	yes
3.2.3.1	Naming, identifier(s)	yes	yes
3.2.3.2	Precise usage	yes	yes
3.2.3.3	Data type, format	yes	yes
3.2.3.4	Classification, coding scheme	yes	yes
3.2.3.5	Range	yes	yes

3.2.3.6	At the attribute level, measures and rules for: contextual data (attribute) relationships, consistency, comparability, continuity, completeness, relevance	yes?	NA
3.2.4	Business Classes (Objects)	yes	yes
3.2.4.1	Naming, identifier(s)	yes	yes
3.2.4.2	Precise usage	yes	yes
3.2.4.3	Relationships with other business objects	yes	yes
3.2.4.4	Aggregated attributes (contained therein)	yes	yes
3.2.4.5	At the class level, measures and rules for: contextual data (attribute) relationships, consistency, comparability, continuity, completeness, relevance	yes?	NA
3.3	Master File: Context Sets/Templates	yes?	NA
3.3.1	Accountability Context	yes?	NA
3.3.2	Data Integrity Context	yes?	NA
3.3.3	Clinical Context	yes	NA
3.3.4	Operational Context	yes	NA
3.4	Master File: Function Definition	yes	NA
3.5	Master File: Security Classification Definition	yes	NA
3.5.1	Classification of information, for aggregations or units of information:		
3.5.1.1	Health records and subsets thereof;	yes	NA?
3.5.1.2	Data groups (datasets);	yes	NA?
3.5.1.3	Attributes (data elements);	yes	NA?
3.5.2	Access permissions for information: e.g., access/use, originate, amend/translate, verify, duplicate, disclose, transmit, receive;	yes	NA?
3.5.3	Classification of functions: for information access, management and processing functions;	yes	NA?
3.5.4	Access permissions for functions: e.g., access, process.	yes	NA?
3.6	Master File: Security Clearance Definition		
3.6.1	Clearances for accountable healthcare parties: individuals, organizations, business units.	yes	NA
3.6.2	Clearances for accountable healthcare roles.	yes	NA
3.7	Master File: Security Policy Domain Definition		NA
3.7.1	Security classifications: for information and functions;	yes	?
3.7.2	Security clearances: for accountable healthcare parties and roles.	yes	NA
3.8	Master File: Orders, Order sets	yes	NA
3.9	Master File: Services, Service Events	yes?	NA
3.10	Master File: Work Flow	?	NA
3.11	Master File: Protocols (Care Plans	yes?	NA

	Critical Paths)		
3.12	Master File: Decision Support Rules, Conditions, Actions	yes?	NA
3.13	Master File: Facilities, Locations	yes?	NA
3.14	Master File: Resources	yes	NA
3.15	Master File: Charges, Costs	yes	NA
4	**Master Registries**	?????	
4.1	Master Registry: Accountable Healthcare Parties		
	For the interchange of registry information, messages (may) include:		
4.1.1	Synchronize, across 2-n registries:	yes	NA
4.1.2	At initial application binding	yes	NA
4.1.3	Dynamic, in real-time	yes	NA
4.1.4	Individual party instance	yes	NA
4.1.5	2-n party instances	?	NA
4.1.6	All party instances in registry	?	NA
4.1.7	Find/match party instance, using identifier(s) and/or trait(s).	?	NA
4.1.8	Update party instance, its identifier(s) and/or trait(s), including actions to: originate, amend/translate.	?	NA
4.1.9	Verify party instance.	?	NA
4.1.10	Activate/deactivate party instance.	?	NA
4.1.11	Enable/disable party's security clearances: for access to information, to functions.	?	NA
4.1.12	Merge/unmerge party instances.	?	NA
4.1.13	List audit trail for party instance.	?	NA
4.1.14	Update audit trail for party instance, including actions to: access, originate, amend/translate, verify, activate/deactivate, enable/disable security clearances, merge/unmerge, transmit, receive.	?	NA
4.1.15	Enable transaction, multi-phase commit: bid, open/lock, update, close/unlock.	yes	NA
4.2	Master Registry: Accountable Healthcare Roles		
4.2.1	Provision, performance and/or completion of health services;	yes	NA
4.2.2	Origination, amendment, stewardship and use of the health record.	yes	NA
	For the interchange of registry information, messages (may) include:		
4.2.3	Synchronize, across 2-n registries:	yes	NA
4.2.4	At initial application binding	yes	NA
4.2.5	Dynamic, in real-time	yes	NA
4.2.6	Individual party instance	yes	NA
4.2.7	2-n party instances	yes	NA
4.2.8	All party instances in registry	yes?	NA
4.2.9	Find/match party instance, using identifier(s) and/or trait(s).	yes?	NA
4.2.10	Update party instance, its identifier(s) and/or trait(s), including actions to:	yes?	NA

	originate, amend/translate.		
4.2.11	Verify party instance.	yes?	NA
4.2.12	Activate/deactivate party instance.	yes?	NA
4.2.13	Enable/disable party's security clearances, for access to information, to functions.	yes?	NA
4.2.14	Merge/unmerge party instances.	?	NA
4.2.15	List audit trail for party instance.	?	NA
4.2.16	Update audit trail for party instance, including actions to: access, originate, amend/translate, verify, activate/deactivate, enable/disable security clearances, merge/unmerge, transmit, receive.	?	NA
4.2.17	Enable transaction, multi-phase commit: bid, open/lock, update, close/unlock.	?	NA
4.3	Master Registry: Accountable Healthcare Agents		
	Essential Characteristic: This messaging/ communication EC specifies the interchange of registry information sufficient to enable a master registry of accountable healthcare agents, including devices and application software. For such interchange, messages (may) include:		
4.3.1	Synchronize, across 2-n registries:	yes	yes
4.3.2	At initial application binding	yes	yes
4.3.3	Dynamic, in real-time	yes	yes
4.3.4	Individual agent instance	yes	yes
4.3.5	2-n agent instances	yes?	?
4.3.6	All agent instances in registry	yes?	?
4.3.7	Find/match agent instance, using identifier(s) and/or trait(s).	yes?	?
4.3.8	Update agent instance, its identifier(s) and/or trait(s), including actions to: originate, amend/translate.	yes?	?
4.3.9	Verify agent instance.	yes?	?
4.3.10	Activate/deactivate agent instance.	yes	yes
4.3.11	List audit trail for agent instance.	?	?
4.3.12	Update audit trail for party instance, including actions to: access, originate, amend/translate, verify, activate/deactivate, transmit, receive.	?	?
4.3.13	Enable transaction, multi-phase commit: bid, open/lock, update, close/unlock.	yes?	?
4.4	Master Registry: Persons (Healthcare Subjects)		
	Essential Characteristic: This messaging/ communication EC specifies the interchange of registry information sufficient to enable a master registry of health subjects, including subjects of care and health plan members. For such interchange, messages (may) include:		
4.4.1	Synchronize, across 2-n registries:	yes	NA
4.4.2	At initial application binding	yes	NA
4.4.3	Dynamic, in real-time	yes	NA
4.4.4	Individual person instance	yes	NA

4.4.5	2-n person instances	yes?	NA
4.4.6	All person instances in registry	yes?	NA
4.4.7	Find/match person instance, using identifier(s) and/or trait(s).	yes	NA
4.4.8	Update person instance, its identifier(s) and/or trait(s), including actions to: originate, amend/translate.	yes	NA
4.4.9	Verify person instance.	yes	NA
4.4.10	Merge/unmerge person instances.	?	NA
4.4.11	Link/unlink person instance to encounter.	?	NA
4.4.12	List audit trail for person instance.	?	NA
4.4.13	Update audit trail for person instance, including actions to: access, originate, amend/translate, verify, merge/unmerge, link/unlink encounters, transmit, receive.	yes	NA
4.4.14	Enable transaction, multi-phase commit: bid, open/lock, update, close/unlock.	yes?	NA
4.5	Local Identifier Assignment Examples:		
4.5.1	Subject of care/health plan member ID: e.g., medical record number	yes	NA
4.5.2	Healthcare professional, employee, user ID	yes	NA
4.5.3	Encounter, episode ID	yes	NA
4.5.4	Financial account ID	?	NA
4.5.5	Location ID	yes	NA?
4.5.6	Equipment, property tag/ID	yes	NA?
4.5.7	Local product ID	?	NA?
5.	**Electronic Records**		
5.1	Personal Health Record	(yes??)	
	Essential Characteristic: This messaging/ communication EC specifies the interchange of the personal health record and its subsets. The personal health record chronicles the health status and interventions for an individual subject of care or health plan member. The information content of the personal health record (may) include: personal identifiers and demographics, environmental, social, financial (e.g., healthcare coverage), allergies, clinical interventions, problems/episodes of care, visits/encounters, personal schedule, consents, disclosures, services received, medication profile, audit, etc. For such interchange, messages (may) include:		
5.1.1	Synchronize, across 2-n health record systems:	(yes)	NA
5.1.2	At initial application binding	(yes)	NA
5.1.3	Dynamic, in real-time	(yes)	NA
5.1.4	Personal health record	(yes)	NA
5.1.5	2-n personal health records	NA	NA
5.1.6	All personal health records	NA	NA
5.1.7	Update audit trails for personal health record interchange: access, amend/translate, transmit, receive	?	NA

5.1.8	Enable interchange based on security classifications, security clearances and data definitions.	(yes)	NA
5.1.9	Enable transaction, multi-phase commit: bid, open/lock, update, close/unlock.	(yes)	NA
5.2	Population Health Record		
	Essential Characteristic: This messaging/ communication EC specifies the interchange of information related to a population health record. For such interchange, messages (may) include:		
5.2.1	Synchronize population health record, across 2-n health record systems.	NA	NA
5.2.2	At initial application binding	NA	NA
5.2.3	Dynamic, in real-time	NA	NA
5.2.4	Update audit trails for population health record interchange: access, amend/translate, transmit, receive.	NA	NA
5.2.5	Enable interchange based on security classifications, security clearances and data definitions.	NA	NA
5.2.6	Enable transaction, multi-phase commit: bid, open/lock, update, close/unlock.	NA	NA
5.3	Business (Operations) Record		NA
	Essential Characteristic: This messaging/communication EC specifies the interchange of information related to a business record. For such interchange, messages (may) include:		
5.3.1	Synchronize business record, across 2-n record systems.	?	NA
5.3.2	At initial application binding	?	NA
5.3.3	Dynamic, in real-time	?	NA
5.3.4	Update audit trails for business record interchange: access, amend/translate, transmit, receive.	?	NA
5.3.5	Enable interchange based on security classifications, security clearances and data definitions.	?	NA
5.3.6	Enable transaction, multi-phase commit: bid, open/lock, update, close/unlock.	?	NA
5.4	Personal Healthcare Professional Service Record	NA	NA
	Essential Characteristic: This Messaging/ communication EC specifies the interchange of information related to a personal healthcare professional service record. For such interchange, messages (may) include:		
5.4.1	Synchronize business record, across 2-n record systems.	NA	NA
5.4.1.1	At initial application binding	NA	NA
5.4.1.2	Dynamic, in real-time	NA	NA
5.4.2	Update audit trails for business record interchange: access, amend/translate, transmit, receive.	NA	NA
5.4.3	Enable interchange based on security classifications, security clearances and	NA	NA

	data definitions.		
5.4.4	Enable transaction, multi-phase commit: bid, open/lock, update, close/unlock.	NA	NA
5.5	Multi-Media Record		
	Example: Electronic health record complete with multi-media content. Formats (may) include:		
5.5.1	Text	yes	NA?
5.5.2	Audio	yes	NA
5.5.3	Video	NA?	NA
5.5.4	Image, graphic	yes	NA
5.5.5	Waveform	yes	NA?
5.5.6	Binary	yes	NA?
6.	**Record Chronology, Continuity, Completeness**		
6.1	Chronological Order of Events		
	Essential Characteristic. This messaging/ communications EC specifies the interchange of information sufficient to describe a chronology of events and corresponding records, for:		
6.1.1	Personal health record	yes	NA
6.1.2	Population health record	NA	NA
6.1.3	Business (operations) record	?	NA
6.1.4	Personal service record	NA	NA
6.2	Event Timeline		
	Essential Characteristic. This messaging/ communications EC specifies the interchange of information sufficient to describe an event timeline.		?
6.2.1	Prospective (future): events scheduled, not yet underway	yes	NA
6.2.2	Concurrent (now): events in progress, not yet completed	yes	NA
6.2.3	Retrospective (historical): events completed, in terminus state	yes	NA
6.3	Historical Snapshot	(yes)	NA
6.4	Continuity, Completeness		
	Essential Characteristic. This messaging/ communications EC specifies the interchange of information sufficient to ensure the continuity and completeness of the health record. Relevant functions may include:		
6.4.1	Completeness metrics: for the health record and its subsets, for data groups (i.e., datasets), attributes (i.e., data elements)	NA?	NA
6.4.2	Gap analysis	?	NA
7.	**Authentication, Non-Repudiation Services**		
7.1	User Authentication.	yes	NA?
7.2	Data Source Authentication	yes	yes
7.3	Validation Authentication.	yes	NA
7.4	Data Interchange Authentication	yes	NA
7.5	Non-Repudiation Services	?	NA
8.	**Digital Signature**		
8.1	Digital Signature	yes	NA

8.2	Public/Private Key Infrastructure (PKI)	?	
9.	**Audit**		
9.1	Audit Trails		
	Essential Characteristic. This messaging/ communications EC specifies the interchange of information sufficient to track the accountable actions of accountable healthcare parties. Audit trails (may) track:		
9.1.1	Provision, performance and/or completion of healthcare services, and specifically health service events: as healthcare professionals and caregivers.	yes	NA
9.1.2	Access to, and use of, health record content.	yes	NA
9.1.3	Origin or amendment of health record content: as authors, scribes.	yes	NA
9.1.4	Verification of health record content.	yes	NA
9.1.5	Duplication of health record content.	yes	NA
9.1.6	Disclosure, transmission or receipt of health record content.	yes	NA
9.1.7	Translation of health record content.	?	NA
9.2	Audit Review	yes	NA
10.	**Permanence, Persistence, Non-Alterability**		
10.1	Permanence, Persistence, Non-Alterability		
	Essential Characteristic. This message/ communications EC specifies interchange of information sufficient to ensure the permanence, persistence and non-alterability of the health record. Relevant functions (may) include:		
10.1.1	Preservation of the health record and its subsets, data groups and attributes	yes	NA
10.1.2	Non-alterability of content	yes	NA
10.1.3	Formal amendment process, preserving previous content	yes	NA
10.1.4	Data state preservation: initial and through each amendment	yes	NA
11.	**OLTP - On-Line Transaction Processing**		
11.1	Tightly Coupled OLTP Services	?	NA
11.2	Multi-Phase Commit	?	NA
12.	**OLAP - On-Line Analytical Processing**		
12.1	OLAP	?	NA
13.	**Fault Tolerance**		
13.1	Redundant Communications Architecture	(yes)	NA
13.2	Unavailability/Failure Detection	yes	yes?
13.3	Availability/Restart Detection	yes	yes?
13.4	Downtime and Slow Response Queuing	?	NA
13.5	Recovery	yes	NA?
14.	**Data Synchrony**		
14.1	Data Synchronization		

	communications EC specifies the interchange of information sufficient to ensure the logical synchronization of information and data stores across communicant applications, components and devices:		
14.1.1	At the initial binding	yes	yes?
14.1.2	At restart	yes	yes?
14.1.3	Continuously in normal operation	yes	yes?
15.	**Time Synchrony**		
15.1	Time Synchrony		
	Essential Characteristic. This messaging/ communications EC specifies the interchange of information sufficient to maintain, within an agreed tolerance, time synchrony across communicant applications, components and devices:		
15.1.1	At initial binding	yes	yes
15.1.2	At restart	yes	yes
15.1.3	At routine intervals in normal operation	yes	yes?
16.	**Trusted End-to-End Information Flows**		
16.1	Trusted End-to-End Information Flows	yes	
	Essential Characteristic. This messaging/ communications EC is based on an architecture sufficient to ensure trusted end-to-end information flows, from the point of origination (point of service/care) to the point of use. In the course of such flow, information may traverse:		
16.1.1	One or more points of interchange: i.e., interfaces between applications/devices	yes	yes
16.1.2	One or more points of translation: e.g., where content is translated from one coding/classification scheme to another	yes?	NA
16.1.3	One or more points of convergence: e.g., where aggregation, derivation or summarization may occur	?	NA
16.2.	End-to-End Record Audit		
	Essential Characteristic. This messaging/ communications EC specifies the interchange of information sufficient to reliably audit its flow from the point of origin to the point of use, tracking accountable actions of accountable healthcare parties/agents. Key audits (may) include:		
16.2.1	Provision, performance and/or completion a health service event (often the sentinel trigger event from Which information flows)	yes	NA
16.2.2	Access to, and use of, the health record or information	yes	NA
16.2.3	Origin or amendment of the health record or information	yes	NA
16.2.4	Verification of health record or information	?	NA
16.2.5	Duplication of health record or information	yes	NA

16.2.6	Disclosure, transmission or receipt of health record or information	yes	NA
16.2.7	Translation of health record or information	?	NA
16.2.8	Stewardship of health record or information (i.e., data at rest)	?	NA
16.3	Chain of Custody Audit	yes?	NA
16.4	Context Sets, Templates		NA
	Examples: Templates which persist from the point of record origin (point of service/care) to the point of use. Templates describing the essential context of a clinical service event:		
16.4.1	Accountability Context, describing:		
16.4.1.1	Who, what, when, where, why, how	yes	NA
16.4.2	Data Integrity Context, describing rules, measures and indicators for information/data:		
16.4.2.1	Accuracy	?	NA
16.4.2.2	Context	?	NA
16.4.2.3	Comparability, consistency	?	NA
16.4.2.4	Continuity, completeness	?	NA
16.4.2.5	Relevance	?	NA
16.4.3	Clinical Context, describing:		
16.4.3.1	Rationale	?	NA
16.4.3.2	Clinical parameters	yes	NA
16.4.3.3	Clinical context and conditions	yes	NA
16.4.3.4	Measures of continuity and completeness (e.g., of the clinical service event)	?	NA
16.4.3.5	Measures of compliance (e.g., with standards of care/practice)	?	NA
16.4.3.6	Performance measures	?	NA
16.4.3.7	Quality indicators	?	NA
16.4.3.8	Outcome indicators	yes	NA
16.4.4	Operational Context, describing:		
16.4.4.1	Allocation, deployment	yes	NA
16.4.4.2	Assigned responsibility	yes	NA
16.4.4.3	Resource utilization (e.g., for staff, time, facilities, equipment, supplies)	yes	NA?
16.4.4.4	Costs	yes???	NA
16.4.4.5	Productivity	??	NA
17.	**Disclosure, Export**		
17.1	Disclosure Authorization, Scope		
	Essential Characteristic. This message/ communications EC specifies interchange of information sufficient to track authorizations for disclosure. Authorization functions (may) include:		
17.1.1	Subject of care authorization for release of information		NA
17.1.1.1	Scope of information eligible for disclosure	?	NA
17.1.1.2	To whom	?	NA
17.1.1.3	For what purpose	?	NA
17.1.1.4	For what duration	?	NA
17.2	Controlled Disclosure Tracking		

	Essential Characteristic. This message/ communications EC specifies interchange of information sufficient to track actual disclosure of sensitive or protected content. Services (may) include:		
17.2.1	Disclosure, transmittal audits	yes	NA
17.2.2	Receipt audits	yes	NA
17.3	Disclosure Labelling	?	NA
17.4	Dis-identification, Aliasing		NA
	Essential Characteristic. This message/ communications EC specifies interchange of information sufficient to ensure dis-identification or aliasing of data exports. Related services (may) include purging or aliasing of:		
17.4.1	Identifiers for individuals, organizations, business units	?	NA
17.4.2	Personal demographics and traits	?	NA
17.4.3	Sensitive/protected information related to		NA
17.4.3.1	Individual subjects of care, health plan members	?	NA
17.4.3.2	Individual healthcare professionals, caregivers	?	NA
17.4.3.3	Organizations, business units	?	NA
18.	**Prospective Services**		
18.1	Subject of care Schedule		
	Essential Characteristic. This message/ communications EC specifies interchange of information sufficient to enable a prospective health schedule for Subjects of care and health plan members. Schedule features (may) include:		
18.1.1	Integrated schedule across multiple care disciplines, business units: departments, services, specialties	NA	NA
18.1.2	Integrated schedule encompassing all venues and encounter types: inpatient, emergent, ambulatory, long-term care, home care	NA	NA
18.1.3	Timeline based, including upcoming clinical service events	yes	NA
18.1.4	Wellness and follow up events	NA	NA
18.1.5	Initiated by healthcare professional orders, order sets	yes	NA
18.1.6	Initiated by protocols: care plans, critical paths	?	NA
18.1.7	Medication profile, medication events	yes	NA
18.2	Assigned Responsibility		
	Essential Characteristic. This message/ communications EC specifies interchange of information sufficient to enable assigned responsibility for scheduled clinical service events, based on business and clinical practice rules. Assignment features (may) include:		
18.2.1	Assignments to specific to individual practitioners	yes	NA
18.2.2	Assignments to a healthcare group	yes	NA

18.2.3	Assignments to a healthcare role	yes	NA
18.3	Healthcare professional Schedule		
	Essential Characteristic. This message/ communications EC specifies interchange of information sufficient to enable a prospective schedule for healthcare professionals, caregivers, groups and roles. Schedule features (may) include:		
18.3.1	Timeline based, including upcoming events	yes	NA
18.3.2	Assigned responsibility	?	NA
18.3.3	Business and clinical rules based	NA	NA
18.4	Resource Schedule		
	Essential Characteristic. This message/ communications EC specifies interchange of information sufficient to enable a prospective resource-based schedule. Schedule features (may) include:		
18.4.1	Business and clinical rules based	NA	NA
18.4.2	Resource factors:		NA
18.4.2.1	Facilities, locations	NA	NA
18.4.2.2	Staff resource factors	NA	NA
18.4.2.3	Time resource factors	NA	NA
18.4.2.4	Equipment resource factors	NA	NA
18.4.2.5	Supply resource factors	NA	NA
18.4.3	Review options:		
18.4.3.1	By individual subject of care	NA	NA
18.4.3.2	By individual healthcare professional	NA	NA
18.4.3.3	By healthcare group or role	NA	NA
18.4.3.4	Across/by organization or business unit: department, service, specialty	NA	NA
18.4.3.5	By resource: facility, location, equipment	NA	NA
18.5	Projections Examples:		
18.5.1	Cost projections	(yes)	NA
18.5.2	Resource projections: facilities, locations, staff, time, equipment, supplies	?	NA
	Essential Characteristic. This message/ communications EC specifies interchange of information sufficient to enable key operational projections, on a prospective basis. Services (may) include:		
18.5.3	Optimal allocations, deployments	NA	NA
18.5.4	Business and clinical rule based	NA	NA
19.	**Work Flow**		
19.1	Work Flow		
	Essential Characteristic. This message/ communications EC specifies interchange of information sufficient to enable and track operational workflow. Work flow features (may) include:		
19.1.1	Real-time, interactive work flow management	?	NA
19.1.2	Shared work flow management:		NA
19.1.2.1	Across organizational boundaries	NA	NA

	professionals, groups		
19.1.2.2	Across and among disciplines, business units	NA	NA
19.1.2.3	Across multiple venues and encounter types: inpatient, emergent, ambulatory, long term care, home care	NA	NA
19.1.3	Based on tight integration of prospective schedules: patient, practitioner, resource	NA	NA
19.1.4	Allocation, deployment of critical resources: facilities, locations, staff, time, equipment, supplies, etc.	NA	NA
19.1.5	Work flow services:		
19.1.5.1	Initiate, assign	?	NA
19.1.5.2	Allocate, deploy (resources)	?	NA
19.1.5.3	Condition	?	NA
19.1.5.4	Stage, sequence, route	?	NA
19.1.5.5	Track, checkpoint, status	?	NA
19.1.5.6	Complete	?	NA
19.1.6	Initiation		
19.1.6.1	By orders, order sets	?	NA
19.1.6.2	By protocols: care plans, critical paths	?	NA
19.1.7	Threading		
19.1.7.1	Single-threaded work flow: tasks in sequence	NA?	NA
19.1.7.2	Multi-threaded work flow: tasks in parallel	NA?	NA
19.1.8	Inter-dependencies: tightly coupled tasks	NA?	NA
19.1.9	Based on business and clinical practice rules	NA?	NA
19.2	Continuity, Completeness		
	Essential Characteristic. This message/ communications EC specifies interchange of information sufficient to ensure the continuity and completeness of work flow and the corresponding healthcare delivery process. Services (may) include:		
19.2.1	Completeness metrics	NA	NA
19.2.2	Continuity monitors, from initiation through completion	?	NA
19.2.3	Gap analysis	?	NA
20.	**Concurrent Status, Records**		
20.1	Concurrent Subject of care Status		
	Example: Real-time, subject of care-centered tracking: e.g.,		
20.1.1	Current health status	yes	NA
20.1.2	Current problems, symptoms, diagnoses	yes	NA
20.1.3	Personal schedule of upcoming events	(yes)	NA
20.1.4	Events in progress, status	yes	NA
20.1.5	Current problem-oriented episodes, active problem list, milestones, status	?	NA
20.1.6	Current protocols (e.g., care plans, critical paths): status, milestones, variances	?	NA
20.1.7	Current encounters, visits	NA	NA

20.1.8	Current medications	yes	NA
20.1.9	Current diagnostics, results	yes	NA
20.1.10	Currently assigned healthcare professionals, caregivers	?	NA
20.2	Concurrent Healthcare Professional Status	?	NA
21.	**Retrospective Status, Records**		
21.1	Retrospective Subject of care Record	yes	
	Example: Real-time, subject of care-centered history:		
21.1.1	Previous health status	yes	NA
21.1.2	Previous problems, symptoms, diagnoses	yes	NA
21.1.3	Events complete, in terminus status	yes	NA
21.1.4	Previous problem-oriented episodes	yes	NA
21.1.5	Previous protocols (e.g., care plans, critical paths): milestones, variances	?	NA
21.1.6	Previous medications	yes	NA
21.1.7	Previous diagnostics, results	yes	NA
21.1.8	Previously assigned healthcare professionals, caregivers	yes	NA
22.	Personal Healthcare Professionals Services		
22.1	Personal Healthcare Professional Portal		
	Essential Characteristic. This message/ communications EC specifies interchange of information sufficient to support a personalized healthcare professional portal. Personal healthcare professional portal services (may) include:		
22.1.1	Assigned responsibilities, incomplete work list: personal or for affiliated healthcare group	?	NA
22.1.2	Action items (e.g., items requiring signature)	?	NA
22.1.3	Notifications, prompts, alerts, reminders	yes	NA
22.1.4	E-mail functions	NA	NA
22.1.5	Significant, un-reviewed events since last access (e.g., new critical results)	?	NA
22.1.6	Based on personalized criteria	?	NA
22.2	Personalized Functions		NA
	Example: Based a healthcare professional's own criteria, personal:		
22.2.1	Views of the health record and its subsets	yes	NA
22.2.2	Orders, order sets	yes	NA
22.2.3	Protocols	yes	NA
22.2.4	Decision support, decision agents	yes	NA
23.	**Data Integrity**		
23.1	Data Integrity		
	Essential Characteristic. This message/ communications EC specifies interchange of information sufficient to ensure data integrity. Data integrity services (may) include:		
23.1.1	Uniform data definition, at various levels of data granularity	yes	yes

23.1.1.1	Public data registry (e.g., USHIK)	(yes?)	yes
23.1.1.2	Health record and its subsets	yes	yes?
23.1.1.3	Data groups (i.e., datasets)	yes	yes
23.1.1.4	Attributes (i.e., data elements)	yes	yes
23.1.2	Measures and indicators for accuracy, context, consistency, comparability, continuity, completeness, relevance	?	NA
23.1.3	Systematic, uniform data capture	yes	NA
23.1.4	Consistent, structured content	yes	NA?
23.1.5	Consistent vocabulary, coding and classification	yes	yes
24.	**Protocols: Care Plans, Critical Paths**		
24.1	Protocol Basis	?	
	Essential Characteristic. This message/ communications EC specifies interchange of information sufficient to enable protocol customisation.		
24.2	Protocol Management	?	
24.2.1	Immediate, interactive review of protocol status: by individual subject of care, health plan member	?	NA
24.2.2	Real-time protocol variance monitor	?	NA
24.2.3	Protocol override, variance authorization	?	NA
	Essential Characteristic. This message/ communications EC specifies interchange of information sufficient to enable real-time protocol management.		
25.	**Problem Lists**		
25.1	Problem List Management		
25.1.1	Immediate, interactive review of current problem list: by individual subject of care, health plan member	yes	NA
25.1.2	Current problem definition, status, milestones	yes	NA
25.1.3	Current problem in terms of corresponding protocols: care plans, critical paths	?	NA
25.1.4	Current problem in terms of assigned responsibilities	?	NA
25.1.5	Review of previous problems: problem, milestones, final resolution/status	yes	NA
26.	**Decision Support**		
26.1	Decision Support Services		
	Essential Characteristic. This message/ communications EC specifies interchange of information sufficient to enable decision support. Services (may) include:		
26.1.1	Based on:		
26.1.1.1	Business and clinical practice rules	yes	NA
26.1.1.2	Practice guidelines, standards of care	yes	NA
26.1.1.3	Protocols	yes	NA
26.1.1.4	Performance measures	?	NA
26.1.1.5	Outcome indicators	yes	NA
26.1.1.6	Cost parameters	?	NA

26.1.2	Detection of:		
26.1.2.1	Duplicate/redundant clinical services	?	NA
26.1.2.2	Conflicts and interactions	?	NA
26.1.3	Real-time, concurrent decision support		
26.1.3.1	At the point of service/care	?	NA
26.1.3.2	At the point of completion of clinical service events: e.g., results, interventions, observations	?	NA
26.1.4	Retrospective decision support: e.g., data warehousing	?	NA
26.1.5	Condition predicated actions, to:	?	
26.1.5.1	Initiate notifications, prompts, alerts, reminders	yes	NA
26.1.5.2	Initiate orders, order sets	?	NA
26.1.5.3	Initiate, revise protocols	?	NA
26.1.5.4	Initiate, cancel, hold clinical service events	?	NA
26.1.6	Link decision support based actions into health record	?	NA
27.	**Surveillance, Metrics and Analysis**		
27.1	Measures and Indicators		
	Example:		
27.1.1	Definitions, rules, measures and indicators for clinical aspects, including:		
27.1.1.1	Continuity, completeness: of the health or operations record, of work flow and the health delivery process	?	NA
27.1.1.2	Compliance: e.g., with standards of practice/care	?	NA
27.1.1.3	Performance, effectiveness	?	NA
27.1.1.4	Quality	?	NA
27.1.1.5	Outcomes	?	NA
27.1.1.6	Protocols, variances	?	NA
27.1.2	Definitions, rules and measures and indicators for operational aspects, including:		
27.1.2.1	Allocation, deployment	?	NA
27.1.2.2	Assigned responsibility	?	NA
27.1.2.3	Resource utilization: facilities, locations, staff, time, equipment, supplies	?	NA
27.1.2.4	Costs		NA
27.1.2.5	Productivity, workload	?	NA?
	Essential Characteristic. This message/ communications EC specifies interchange of information sufficient to enable definitions, rules, measures and indicators with regard to aspects of clinical and operational performance and quality.		
27.2	Epidemiological Surveillance	yes?	NA
	Essential Characteristic. This message/ communications EC specifies interchange of information sufficient to enable epidemiological surveillance.		
28.	**Communications Infrastructure**		
28.1	Communications Infrastructure		

	Essential Characteristic. This message/ communications EC specifies interchange of information sufficient to ensure timely and reliable information conveyance. Services (may) include:		
28.1.1	Real-time, immediate information conveyance: e.g., point of origination (point of service/care) to point of use	yes	yes
28.1.2	Notifications, prompts, alerts, reminders	yes	yes?
28.1.3	E-mail functions	NA?	NA
28.1.4	Telephone replacement functions	NA?	NA
28.1.5	Paper replacement functions	yes	NA
28.1.6	Affirmative acknowledgment of receipt: by individual practitioners, caregivers	?	NA
29.	**Multiple Person Linkage**		
29.1	Multiple Person Linkage		NA
	Examples of logical person linkages:		
29.1.1	Next of kin	?	NA
29.1.2	Mother/child	?	NA
29.1.3	Multiple birth, including sequence	?	NA
29.1.4	Guarantor, guarantee	NA	NA
29.1.5	Insured, subscriber, health plan member	NA	NA
29.1.6	Emergency contact(s)	yes	NA
	Essential Characteristic. This message/ communications EC specifies interchange of information sufficient to enable the logical linkage of multiple persons.		
30.	**Subject of care – Healthcare Professional Linkage**		
30.1	Healthcare Professional, Subject of care Linkage	yes?	NA
	Essential Characteristic. This message/ communications EC specifies interchange of information sufficient to enable the logical linkage of subjects of care and healthcare professionals.		
31.	**Localization, Local Authority**		
31.1	Localization		?
	Essential Characteristic. This message/ communications EC specifies interchange of information sufficient to enable localization. Localization (may) include:		
31.1.1	Security, access control:	yes	
31.1.1.1	Security policies, policy domains	yes	NA?
31.1.1.2	Classifications: functions, information	yes	NA?
31.1.1.3	Clearances: users, roles	yes	NA?
31.1.2	Identifiers	yes	yes?
31.1.3	Accountable healthcare parties, agents	yes	?
31.1.4	Accountable healthcare roles	yes	NA?
31.1.5	Accountable healthcare groups	yes	NA?
31.1.6	Data definitions: health record and its subsets, data groups, attributes	yes	NA?
31.1.7	Context sets, templates	yes	NA?
31.1.8	Business and clinical practice rules	yes	NA
31.1.9	Practice guidelines, standards of care	yes	NA
31.1.10	Orders, order sets	yes	NA

31.1.11	Services, service events	yes	NA?
31.1.12	Work flow	yes?	NA
31.1.13	Protocols: care plans, critical paths	yes?	NA
31.1.14	Decision support rules, conditions, actions	yes?	NA
31.1.15	Facilities, locations	yes	NA?
31.1.16	Charges, costs	NA?	NA
31.1.17	Surveillance, metrics and analysis: rules, measures and indicators etc.	?	?
32.	**User Environments**		
32.1	User Environments		
	Examples of user environments:		
32.1.1	Production	?	?
32.1.2	Test, development	?	?
32.1.3	Education, training	?	?
	Essential Characteristic. This message/ communications EC specifies interchange of information sufficient to support discrete user environments		
33.	**Version Management**		
	Examples of versioned constructs:		
33.1	Application, component or device software	yes	
33.1.1	Vocabulary: coding, classification schemes	yes	yes
33.1.2	Master definition files	yes	?
33.1.3	API standards	yes	?
33.1.4	Message, EDI standards: i.e., level 7	yes	yes ?
33.1.5	Network, communications standards: i.e., levels 1-6	yes?	yes
	Essential Characteristic. This message/ communications EC specifies interchange of information sufficient to enable version management and rollover to new revisions.		
34.	**Inter-Application**		
34.1	Application Roles	?	yes
	Essential Characteristic. This message/ communications EC specifies interchange of information sufficient to enable specific application/component roles, as explicitly described.		
34.2	Application Interactions		yes
	Essential Characteristic. This message/ communications EC specifies interchange of information sufficient to support typical application/component interaction paradigms. Relevant paradigms (may) include:		
34.2.1	Trigger events	yes	yes
34.2.2	Unsolicited updates	yes	yes
34.2.3	Query/response	yes	yes
34.2.4	Receipt acknowledgment	yes	yes
34.3	Inter-Application Relationships	?	
	Essential Characteristic. This message/ communications EC specifies interchange of		

	information sufficient to enable typical inter-application/component relationships. Relevant relationships (may) include:		
34.3.1	Point to point interaction model: paired sender/receiver	yes	yes
34.3.2	Inter-dependencies	?	?
34.4	Inter-Application Services		
	Essential Characteristic. This message/ communications EC specifies interchange of information sufficient to enable typical inter-application/component services. Services (may) include:		
34.4.1	API: tightly coupled, passed parameters	yes	
34.4.2	Message: loosely coupled (e.g., EDI/EDIFACT, HL7, DICOM, MIB)	yes	yes
34.4.3	Mediated message interchange (e.g., via interface engines, hubs)	yes	yes
34.4.3.1	En-route queuing, store and forward	?	NA
34.4.3.2	En-route translation, transformation: of data groups, of attributes	yes	NA
34.4.3.3	Phase I acknowledgment: mediator to transmitter	?	?
34.4.3.4	Phase II acknowledgment: receiver to mediator	?	?
34.4.3.5	End-to-end acknowledgment: receiver to transmitter	yes	yes
34.4.3.6	Phase I threaded message sequence: transmitter to mediator	?	?
34.4.3.7	Phase II threaded message sequence: mediator to receiver	?	?
34.4.3.8	End-to-end threaded message sequence: transmitter to receiver	?	?
34.4.4	Security, access control	yes	?
34.4.5	Audit	yes	?
34.4.6	Clock synchrony	yes	yes
34.4.7	Data synchrony	yes	yes ?
34.4.8	Transactions, multi-phase commits (to synchronous data stores)	yes	NA
34.4.9	Data definition	yes	yes
34.4.10	Master files	yes	?
34.4.11	Master registries	yes	?
35.	**Change Scale**		
35.1	Change Scale	yes	NA
	Essential Characteristic. This message/ communications EC specifies interchange of information sufficient to enable broad extensibility and change of scale of health record systems and the environments they support.		
36.	**Validation**		
36.1	Validation	yes	yes
	Essential Characteristic. This message/ communications EC has evidenced substantial, broad-based validation in the environments to which it is targeted and in terms of the purposes for which it is intended.		